Planning for Information System Security

“Speak English!” said the Eaglet. “I don’t know the meaning of half those long words, and what’s more, I don’t believe you do either!”

The Red Queen said, “Now, here, it takes all the running you can do to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!”

—Lewis Carroll, Alice in Wonderland

Over the past several months Joe Dawson had really immersed himself in the subject of security. However, the more he read and talked to the experts, the more confused he became. Clearly, Joe felt, something was not right. After all, managing security should not be that difficult. In terms of his own business, Joe had really worked hard to be at a point where his business was rather successful. So, managing security should not be that tough. He was after all qualified and competent. But on most occasions Joe got lost in the mumbo jumbo of terminology, which made it quite impossible to make sense of anything.

As Joe considered the complexities of security and its implementation in his organization, he was reminded of a book he had read while in the MBA program—The Deadline by Tom DeMarco. This was an interesting book that presented principles of project management in a succinct manner. In particular, Joe remembered something about processes for undertaking software development work. He reached out for the book and began flipping through the pages. Aah! It was there on page 115. There were four bullet points on developing processes:

• Model your hunches about the processes that get work done.

• Use the models in peer interaction to communicate and refine thinking about how the process works.

• Use the models to simulate results.

• Tune the models against actual results.

Wasn’t the advice given by DeMarco so very true for any organization, any implementation? Joe thought for a moment. Clearly security management was about identifying the right kind of process and ensuring that it works. This means that he had to think proactively about security, plan for it, and have the right process in place. If the business process had been sorted out, wouldn’t that result in a high-integrity operation? Wasn’t high integrity a cornerstone of good security? It all seemed to fall into place. Maybe he had started at the wrong place by focusing on the technological solutions, Joe thought. Maybe security was not about technology at all. At this point Joe was interrupted by a phone call.

It was Steve, who lived four houses down the lane. Both Steve and Joe were Lakers fans. After discussing Lakers strategies to get back the key position player, Steve asked, “Do you have a wireless router?” “Yes,” said Joe. “I think I am picking up your signal. You need to secure it.” After all, understanding technology was important, Joe thought instantly. Joe did not know how to fix the problem. And Steve volunteered to come over and help Joe out.

Although the wireless router problem got resolved, Joe was still uncomfortable with strategizing about security at SureSteel. Should he sit down with his technology folks and write a security policy? Should he simply let the policy emerge in a few years? How was he going to deal with other companies and assure that his systems were good enough? Was there any need to do so? These were all very true and genuine questions. Joe understood the nature and significance of these questions. He had been formally trained to appreciate and deal with these issues. Joe knew that these issues and concerns were indeed the building blocks of the strategy process. Henry Mintzberg had written a wonderful article in California Management Review in 1987, which Joe remembered and knew was still relevant. Mintzberg had conceptualized strategy in terms of five Ps—plans, ploys, patterns, positions, perspectives.

Strategy as a plan is some sort of a consciously intended course of action. Joe knew that any security plan he initiated at SureSteel was going to be formally articulated. Strategy could also be a ploy. In this case specific “maneuvers” to outwit opponents trying to impregnate SureSteel systems would have to be developed. Joe remembered his computer geek friend Randy, who had said that maintaining security of systems is like a “Doberman awaiting intruders.” In many ways, Joe thought, a ploy is a deterrent strategy.

Joe was also responsive to Mintzberg’s conceptualization of strategy as a pattern. Clearly it is virtually impossible for SureSteel to identify and establish countermeasures for all possible threats. What Joe had to do was identify patterns that might exist as the organization went about doing its daily business. The dominant patterns that might emerge would form the basis for any further learning and strategizing that Joe might be involved in.

In his pursuit to achieve a good strategic vision for SureSteel, Joe did not want to create security plans that would hinder the job of his employees. After all, security is a key enabler for running a business smoothly. Such a conception suggests that strategy is a position—a position between the organization and the context, and between the day-to-day activities of the company and its environment. Clearly a perspective has to be developed. A strategic security perspective would allow for a security culture to be developed, allowing all employees to think alike in terms of maintaining security.

Such thinking was helping Joe to consider multiple facets of security. All he needed was a means to articulate and structure the thinking.

Formal IS security is about creating organizational structures and processes to ensure security and integrity. Since organizing is essentially an information handling activity, it is important to ensure that the proper responsibility structures are created and sustained, integrity of the roles is maintained, and adequate business processes are created and their integrity established. Furthermore, an overarching strategy and policy needs to be established. Such a policy ensures that the organization and its activities stay on course.

Various IS security academics and practitioners have identified the need to understand formal IS security issues. The call for establishing organizationally grounded security policies has been made by numerous researchers and practitioners. One of the earlier papers to make such a call, and published in Computers & Security, was in 1982. Entitled “Developing a Computer Security and Control Strategy,” the paper focused on establishing appropriate security strategies. The author, William Perry, argues that a computer security and control strategy is a function of establishing rules for accessibility of data, processes for sharing business systems, and adequate system development practices and processes. Perry also identifies other issues such as competence of people, data interdependence rules, etc. [15]. The arguments proposed in his article are indeed relevant even today.

More than two decades later, in another interesting paper published in Computers & Security, Basie von Solms and Rossouw von Solms presented the 10 deadly sins of information system security management [18]. Central to their argument is the importance of structures, processes, governance, and policy. The authors note that information system security is a business issue, and security problems cannot be dealt with by just adopting a technical perspective. Therefore although it’s important to establish system access criteria and technical means to secure systems, these will perhaps not work or will fail if adequate organizational structures have not been put in place. A summary of the 10 deadly sins postulated by Solms and Solms appears in Table 5.1.

The 10 deadly sins identified by Solms and Solms essentially suggest four classes of formal IS security issues. These include:

• Security strategy and policy—development of a security strategy and policy that would determine the manner in which administrative aspects of IS security are managed.

• Responsibility and authority structures—a definition of organizational structures and how subordinates report to superiors. Such a definition helps in establishing access rules to systems.

• Business processes—defining the formal information flows in the organization. Information flows have to match the business processes in order to ensure integrity of the operations.

• Roles and skills—identifying and retaining the right kind of people in organizations is as important as defining the security policy, structures, and processes.

Table 5.1. 10 deadly sins of IS security management [18]

Deadly sins of information system security

1. Not realizing that information security is a corporate governance responsibility (the buck stops right at the top)

2. Not realizing that information security is a business issue and not a technical issue

3. Not realizing the fact that information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single “off the shelf” solution)

4. Not realizing that an information security plan must be based on identified risks

5. Not realizing (and leveraging) the important role of international best practices for information security management

6. Not realizing that a corporate information security policy is absolutely essential

7. Not realizing that information security compliance enforcement and monitoring is absolutely essential

8. Not realizing that a proper information security governance structure (organization) is absolutely essential

9. Not realizing the core importance of information security awareness amongst users

10. Not empowering information security managers with the infrastructure, tools, and supporting mechanisms to properly perform their responsibilities

Formal IS Security Dimensions

There can possibly be a number of security dimensions in the formal parts of an organization. These are identified and discussed below.

Responsibility and Authority Structures

When responsibility and authority structures are ill-defined or not defined at all, it results in a breakdown of the formal controls systems. Clearly adopting adequate structures will go a long way in establishing good management practices and will set the scene for effective computer crime management. The notion of structures of responsibility goes beyond the narrowly focused concerns of specifying an appropriate organizational structure. Although important, exclusive focus on organizational structure issues tends to skew the emphasis towards formal specification. In a 1996 paper, Backhouse and Dhillon [3] introduced the concept of structures of responsibility to the information system security literature. They suggest that responsibility structures provide a means to understand the manner in which responsible agents are identified within the context of the formal and informal organizational environments. The most important element of interpreting structures of responsibility is the ability to understand the underlying patterns of behavior.

Backhouse and Dhillon evaluate issues and concerns related to interpreting structures of responsibility. Their inherent argument is that the organizational structures are manifestations of the roles and reporting structures of organizational members. It is for this reason that any organizational structure should be modeled on the basis of understanding the communication necessary for achieving a coordinated action. After all, an organizational structure is a means to achieve a coordinated outcome. With respect to security, Backhouse and Dhillon argue that understanding the communication flows and identifying places where the communication might break down allows an assessment of IS security. They further argue that usually security problems are a consequence of communication breakdowns and lack of understanding of behaviors of various stakeholders. The structures of responsibility provide a means to understand the manner in which responsible agents are identified; the formal and informal environments in which they exist; the influences they are subjected to; the range of conduct open to them; the manner in which they signify the occurrence of events; the communications they enter into; and, above all, the underlying patterns of behavior.

Box 5.1. Data Stewardship

One way in which responsibility and authority structures have been manifested in organizations is through the role of a data steward. Many companies now have this role as part of their organizational structure.

The data steward role is primarily responsible for data quality. Although uncommon in smaller organizations, most large companies are recognizing the importance of data quality and ensuring that someone in the company is in charge. Although there is a movement in the industry that emphasizes the importance of data quality, there are many organizations that essentially dwell within the “find-and-fix” paradigm, usually undertaken after a project has been completed. A typical corporate data stewardship role may have one data steward assigned to each major data subject area. Such individuals may not carry the title of a data steward, but may nevertheless perform the functions typical of maintaining data quality.

Typically, data stewards manage data assets to improve reusability, accessibility, and quality. They may be involved in data naming standards and developing consistent data definitions for documenting business rules. So, in one sense a role such as that of a data steward manifests itself by enforcing organizational hierarchy and business rules. This is an important aspect of this role since it ensures integrity of the operations.

Jonathan Geiger in an article in Teradata Magazine (September 2008), summarizes the requirements of a data steward as follows:

• Business knowledge: Data stewards must understand the business direction, processes, rules, requirements, and deficiencies.

• Business-area respect: They need to influence business decisions and gain business-area commitments.

• Analysis: When faced with multiple options, they must examine situations from many angles.

• Facilitation and negotiation: They must facilitate the proponents of conflicting viewpoints to arrive at a mutually satisfactory solution.

• Communication: Stewards need to effectively convey the business rules and definitions and promote them with the business areas as well.

Organizational Buy-In

The effectiveness of the security policy is a function of the level of support it has from an organization’s executive leadership. Although this may sound obvious, it is indeed the most challenging task. A related challenge is that of educating the employees. It is easier to harden the operating systems and undertake virus scans than it is to communicate security policy tenets to various stakeholders.

There is a two-fold need for executive leadership buy-in. First, it assures staff buy-in. When the executive leadership visibly validates the security policy and procedures, it becomes easier to “sell” the program to organizational staff members. If however the executive leadership does not support the policies and procedures, it becomes difficult, if not impossible, to convince the rest of the organization to adopt the security policy. Second, executive leadership buy-in ensures funding for a comprehensive IS security program.

Support from the IT department for the security policy and procedures is also essential. Consensus needs to be reached regarding the best practices to protect enterprise information assets. There usually are more than one means to establish such protective mechanisms. While it may be important to acknowledge the importance of different approaches, it is equally important to identify the best possible way to achieve security objectives. If the debates on the best possible course of action continue, it can then become detrimental to the overall success of the security policy. If departments themselves cannot agree on the best possible course of action, then support from non-technical staff becomes difficult as well.

User support is another important ingredient. User support resides in the people throughout the organization and represents a critical functional layer that could be rather useful in the overall defense strategy. A strategy of “locks and keys” becomes inadequate if people inside the organization open those locks (i.e. subvert the controls). Once the organizational shortcomings have been identified, the next step is to establish an education and training program.

The National Institute of Standards and Technology (NIST) in their document NIST 800-14 (“Generally Accepted Principles and Practices for Securing Information Technology Systems”) prescribes the following seven steps to be followed for effective security training:

1. Identify program scope, goals, and objectives. The scope of the program should provide training to all types of people who interact with IT systems. Since users need training which relates directly to their use of particular systems, a large organization-wide program needs to be supplemented by more system-specific programs.

2. Identify training staff. It is important that trainers have sufficient knowledge of security issues, principles, and techniques. It is also vital that they know how to communicate information and ideas effectively.

3. Identify target audiences. Not everyone needs the same degree or type of security information to do their jobs. A computer security awareness and training program that distinguishes between groups of people, presents only the information needed by the particular audience, and omits irrelevant information, will have the best results.

4. Motivate management and employees. To successfully implement an awareness and training program, it is important to gain the support of management and employees. Consider using motivational techniques to show management and employees how their participation in a security and awareness program will benefit the organization.

5. Administer the program. Several important considerations for administering the program include visibility, selection of appropriate training methods, topics, materials, and presentation techniques.

6. Maintain the program. Efforts should be made to keep abreast of changes in computer technology and security requirements. A training program that meets an organization’s needs today may become ineffective when the organization starts to use a new application or changes its environment, such as by connecting to the Internet.

7. Evaluate the program. An evaluation should attempt to ascertain how much information is retained, to what extent security procedures are being followed, and general attitudes toward security.

Security Policy

It goes without saying that a proper security policy needs to be in place. Numerous security problems have been attributed to the lack of a security policy. Possible vulnerabilities related to security policies occur at three levels—policy development, policy implementation, policy reinterpretation. Vulnerabilities at the policy development level exist because of a flawed orientation in understanding the range of actual threats that might exist. As will be discussed later in the chapter, security policy formulation that does not consider the organizational vision or is developed in a vacuum often results in it not being adopted. Such policies cause more harm than good. Clearly organizations tend to have a false sense of security due to the policy, thus resulting in ignoring or bypassing the most obvious controls.

Some fundamental issues that could possibly be considered in good security policy formulation include:

1. The strategic direction of the company needs to be incorporated at both micro and macro levels.

2. Clarification of the strategic agenda sets the stage for developing the security model. Such a model identifies the relationship between the business areas and the security policies for that business area.

3. The security policies determine the processes and techniques required to provide the security but not the technology.

4. The implementation of security policies entails the development of procedures to implement the techniques defined in the security policies. The implementation stage defines the nature and scope of the technology to be used.

5. Following the implementation there is a constant need to monitor the security processes and techniques. This enables checks to be made to ascertain effectiveness at three levels: policy, procedure, and implementation. In particular, an assessment is made of the uptake of the security policies; implementation of procedures; detection of breach of procedures. Monitoring also includes assessment and reassessment to ensure that procedures match the original requirements.

6. A response policy is also an integral part of a good security policy. It pre-empts a security failure and determines the impact of a failure at policy, procedure, implementation, or monitoring levels. It is essentially the security breach risk register.

7. Finally, a program is needed to establish procedures and practices for educating and making all stakeholders aware of the importance of security. Staff and users also need to be trained on methods to identify new threats. In the current changing business environment new vulnerabilities constantly keep emerging and it’s important to have the requisite competence to identify and manage them.

An important aspect of the security model is the layered approach. One cannot begin working on any layer without having taken certain prerequisite steps. The design of formal IS security can best be illustrated as layers, shown in Figure 5.1.

To summarize, at a formal level we consider IS security to be realized through maintaining good structures of responsibility and authority. Organizational buy-in and ownership of security by top management are the key success factors in ensuring security. Finally, the importance of security policies cannot be underestimated. A general framework for conceptualizing security policies incorporates three interrelated considerations:

• Organizational considerations related to structures of responsibility for information system security

• Ensuring organizational buy-in for the information system security program

• Establishing security plans and policies and relating them to the organizational vision

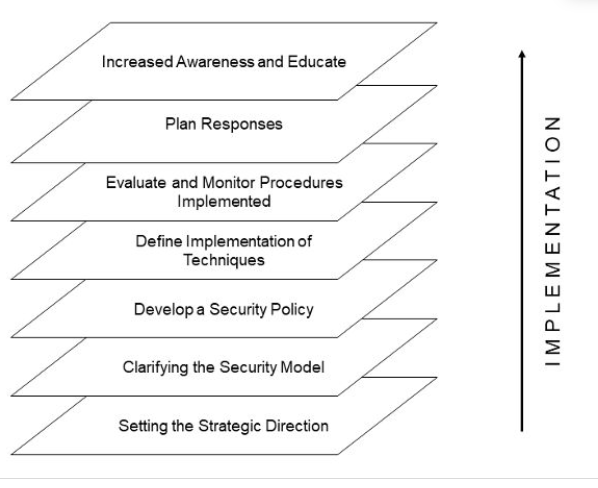


Figure 5.1. Layers in designing formal IS security

Security Strategy Levels

There is often confusion between the various terms—strategy, policy, programs, and operating procedures. The term strategy is used to refer to managerial processes such as planning and control, defining the mission and purpose, identification of resources, critical success factors, etc. Corporate strategy has been considered as the primary means to cope with the environmental changes that an organization faces. It is often considered as a set of policies which guides the scope and direction of an organization. However, there is much confusion between what is designated as a policy and what as strategy. Ansoff [1] (p. 114) traces the origin of the term strategy to “military art, where it is a broad, rather vaguely defined, ‘grand’ concept of a military campaign for application of large-scale forces against the enemy.” In business management practices, the term policy was in use long before strategy but the two are often used interchangeably, despite having very different meanings. In practice, a policy refers to a contingent decision.1 Therefore, implementing a policy can be delegated, while for implementing a strategy executive judgment is required. The term program is generally used for a time-phased action sequence that guides and coordinates various operations. If any action is repetitive and the outcome is predetermined, the term standing operating procedure is used.

In the realm of IS security, it is important to differentiate between these terms since there is much confusion. Clearly there needs to be a strategy as to what needs to be done with respect to security. Such a strategy should determine the policies and procedures. However, in practice rarely is a strategy for security created. Most emphasis is placed on policies, implementation of which is generally relegated to the lowest levels, and it is simply assumed that most people will follow the policy that is created.

If we accept that secure information systems enable the smooth running of an enterprise, then what determines the ability of a firm to protect its resources? There are two routes (Figure 5.2). Either a firm considers security as a strategic issue and hence operates in an environment designed to maintain consistency and coherence in its business objectives, or, a firm may position itself such that it gains advantage in terms of the risks afforded by the environment. This has traditionally been achieved by performing a risk analysis. This demarcation identifies two levels of a strategy within an organization: the corporate and the business level.

At a corporate level the security strategy determines key decisions regarding investment, divestment, diversification, and integration of computing resources in line with other business objectives. The primary concern here is to take decisions regarding the nature and scope of computerization. At a business level, the security strategy looks into the threats and weaknesses of the IT infrastructure. In the security literature many of these issues have been studied under the banner of risk analysis. The manner in which risk analysis is conducted is a subject of much debate, as are the implementation aspects. While a business security strategy defines the overall approach to gain advantage from the environment, the detailed deployment of the procedures at the operational level is an issue of concern for functional strategies (i.e. the security policy). These functional strategies may either specifically target major organizational activities such as marketing, legal, personnel, finance, or may be more generic and consider all administrative elements.

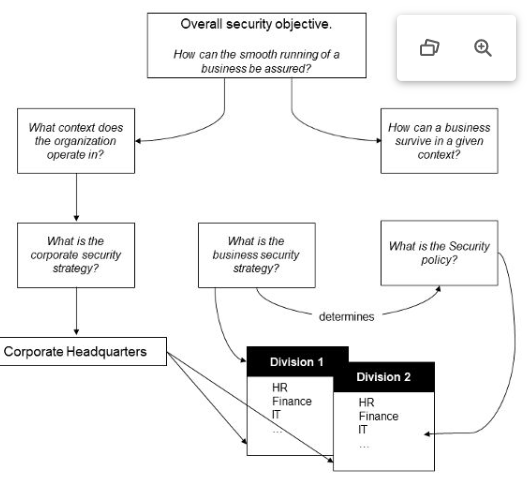


Figure 5.2. Strategy levels

Most of the existing research into security considers that policies are the sine qua non of well-managed secure organizations. However, it has been contended that “good managers don’t make policy decisions” ([19]; p. 32). This avoids the danger of managers being trapped in arbitrating disputes arising out of stated policies rather than moving the organization forward. This does not mean that organizations should not have any security policies sketching out specific procedures. Rather, the emphasis should be on developing a broad security vision that brings the issue of security to center stage and binds it to the organizational objectives. Traditionally, security policies have ignored the development of such a vision, and instead a rationalistic approach has been taken which assumes either a condition of partial ignorance or a condition of risk and uncertainty. Partial ignorance occurs when alternatives cannot be arranged and examined in advance. A condition of risk presents alternatives that are known along with their probabilities. Under uncertainty, alternatives may be known but not the probabilities. Such a viewpoint forces us to measure the probability of occurrence of events. Policies formulated on this basis lack consistency with the organizational purpose.

Classes of Security Decisions in Firms

One of the problems, as discussed in the previous section, relates to relegating IS security decisions to the operational levels of the firm. Inadvertently, this results in lack of ownership by the top management. In most cases this means that the senior management adopts a “hands off” attitude. Such an attitude might work if a firm has little dependence on IT systems. In the current business environment this is rarely the case though. For this reason it is prudent to differentiate between different classes of IS security decisions and to award adequate importance to each of the classes at the relevant levels. Different classes of IS security decisions are presented in Table 5.2 and discussed in the paragraphs below. It should however be noted that these classes are not mutually exclusive. There is obviously a fair amount of overlap, with the core purpose of the security decisions relating to configuring and directing the resource conversion process so as to optimize attainment of objectives. Clearly the main objective with respect to security is to create an environment where there is no scope for abusing the systems and processes.

Strategic Decisions

One of the fundamental problems with respect to security is for a firm to choose the right kind of an environment to function in. Strategic security issues, therefore, relate to where the firm chooses to do its business. If a given firm chooses to set up headquarters in a war-ravaged environment, clearly there will be increased threat to physical security. Or, if a firm chooses to be headquartered in an environment where bribery is rampart, it increases the chances that company executives will engage in unethical acts, which at times may result in subverting existing control structures. Strategic decisions for security can also relate to the nature and scope of a firm’s relationship to other firms and the contexts within which it might choose to operate. For instance, if a firm chooses to integrate its enterprise systems with a US-based firm, it clearly will have to ensure compliance with corporate governance principles as mandated by the Sarbanes-Oxley Act of 2001. Furthermore, any change to an existing business process will have legal implications for either of the partners.

Allocation of resources among competing needs therefore becomes a critical problem in terms of strategizing about security. Apart from high-level corporate governance and firm location issues, which no doubt are important, issues such as return on investment in security products and services become important. IT directors will have to ask some very fundamental questions, such as: Are investments in security products and services paying off? Addressing this issue would have a range of implications for success in ensuring security. Today many managers are asking this question [6]. Indeed, over the past few years investments in security have been going up, but so have the number and range of security breaches. This would mean that perhaps the security mechanisms are not working. Or maybe the security investments are being made in the wrong places. It could also be that the benefit of a security investment is intangible and that it is rather difficult to link a tangible investment in security to a tangible benefit. After all, most security-related investments are triggered by fear, uncertainty, and doubt [16].

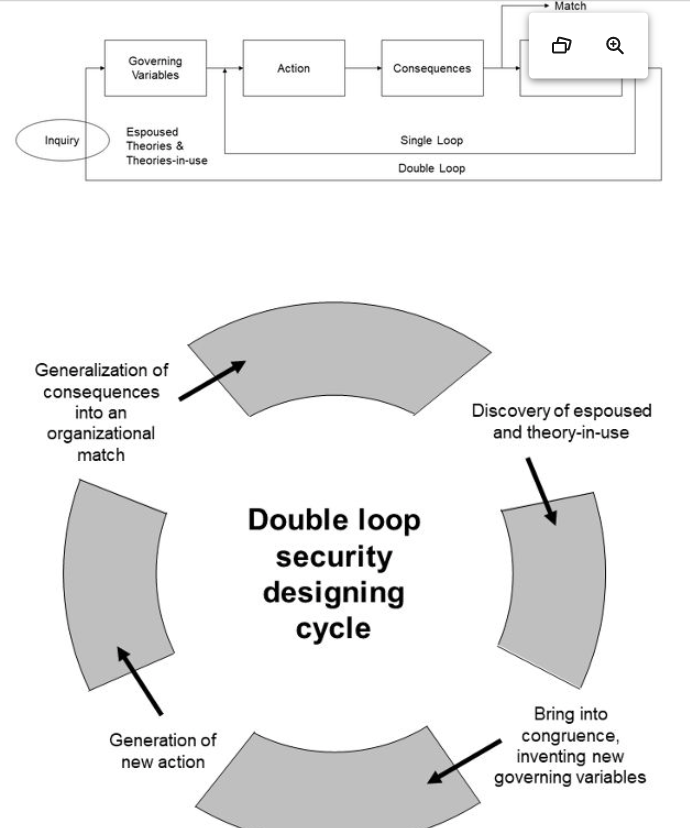


Figure 5.4. Double loop security design process

Administrative Decisions

An understanding of a range of strategic aspects of IS security is clearly an important aspect. Equally important, if not more, is an understanding of structures and processes that should be created to adequately deal with information handling. Inability to properly design structures and processes can be a major reason why many security breaches take place. Usually, design of structures and processes is considered to be beyond the realm of traditional IS security. However, as stated previously, structures and processes are increasingly becoming more central to planning and organizing for security (cf. consequences of the Sarbanes-Oxley Act).

One of the key decisions with respect to structures and processes relates to responsibility and authority. It goes without saying that any organization needs to have in place a process for doing things. If the substantive task at hand is order fulfillment for example, then a business process needs to be created that identifies a range of activities that will be undertaken when the first order comes in. Each of the activities will have information flows associated with it. It is prudent to not only map all the information flows, but also undertake consistency and integrity checks. Obviously redundancy has to be taken care of. Traditionally, mapping of information flows and integrity checks have been done whenever new computer-based systems have been developed. This activity has taken the form of drawing data flows, establishing entity relationships, etc. Use of data flows and entity relationships is not (and should not be) restricted to design and development of new IT solutions. In fact, it is an important task that all organizations should undertake.

While creating processes, associated organizational structures also need to be designed. At the confluence of the processes and structures reside the responsibilities and authorities. In large organizations it is rather difficult to balance the process and structure aspects. As a consequence, responsibilities and authorities never get defined properly. Even if they are, delineation of responsibilities and authorities is invariably not undertaken. Subsequently, when computer-based systems are developed, ill-defined responsibilities and authorities often get reflected in the system. There are two reasons for this. First, the individuals who are usually interviewed by the analysts to assess system requirements occupy roles that have been ill defined. Second, even though the system developed imposes certain structures of responsibility, the mix of business processes and structures is not geared to deal with it.

The issue at hand has been well discussed and studied by a number of researchers and practitioners alike. The cases of Daiwa and Barings Bank have been well researched [11-12, 17]. Dual responsibility and authority structures and their subsequent abuse by Nick Lesson of Barings Bank is an excellent case in point, as is the 2008 Société Générale fiasco because of fraudulent transactions created by Jérôme Kerviel. As has been well documented, Lesson was able to subvert the controls because the structures had not been well defined in the latest round of changes. A similar situation brought about the demise of Daiwa Bank and Kidder Peabody [8].

Decisions related to formal administrative controls deal with establishing adequate business structures and processes so as to maintain high-integrity data flow and the general conduct of the business. Establishing adequate processes also ensures compliance with regulatory bodies, organizational rules and policies. Therefore, it goes without saying, good business processes and structures ensure the safe running of the business and prevent crime from taking place. Clearly, mature organizations have well-established and institutionalized processes and newer enterprises have to engage in the process of innovation and institutionalization. To a large extent high-integrity processes are a consequence of adequate planning and policy implementation.

Some aspects that Dhillon and Moores [8] recommend as immediate steps to ensure that proper responsibilities and authorities are established include:

• Setting standards for proper business conduct

• Monitoring employees to detect deviations from standards

• Implementing risk management procedures to reduce the opportunities for things to go wrong

• Implementing rigorous employee training, instituting individual accountability for misconduct

Another aspect related to administrative decisions is that of facilities management. While most of the organizational security resources get directed to protecting the logical aspects, little consideration is given to the physical aspects and general facilities management. In a study of security infrastructure at a UK-based local authority, Dhillon [5] found that there were absolutely no physical access controls to the server rooms. This was in spite of a significant thrust made toward security. In presenting the findings of the study Dhillon observed:

The hub of the IT department of the Local Council is the Networking and Information Centre. This Centre has a Help Desk for the convenience of the users. At present there is no physical access control to prevent unauthorised access to the Help Desk area and to the Networking and Information Centre. The file servers and network monitoring equipment remains unprotected even when the area is unoccupied. In fact the file servers and network monitoring equipment throughout the Council should be kept in physically secure environments, preferably locked in a cabinet or secure area. This would prevent theft or deliberate damage to the hardware, application software or data on the network. Access to the Help Desk area can typically be restricted by a keypad. The auditors had identified these basic security gaps, but concrete actions are still awaited.

Such behavior on the part of organizations is indeed very common. Lack of consideration of the basic hygiene and simplest controls is often overlooked. To some extent this can be tied back to issues of—Who is responsible? Who has authority? Who is accountable?

Operational Decisions

In most firms there are a myriad of operational problems that require immediate attention. To a large extent such problems can be managed if initial design of work patterns and activities is done with care. This would ensure significant efficiency gains. However, such detailed work flow analysis and review is rarely done. As a consequence, small operational problems end up affecting the administrative and strategic levels as well. Since there is little flexibility and authority in the hands of operational staff, any problem automatically becomes an issue for the top management. The volume of such problems is usually great, essentially because of the need for daily supervision and control.

Although staff at the operational level cannot and should not be given authority to “tweak” the business processes, it is prudent for the higher management to take some key decisions related to identifying operational goals and objectives. If the goals and objectives are clarified, it pretty much sets the stage for establishing operational control strategies and policies and procedures for various functional divisions. Careful planning and establishing proper checks and balances are perhaps the cheapest of the operational level security practices. Once the design for various procedures has been adequately undertaken, it helps in identifying the range of relevant security initiatives.

The premise on which operation decisions are taken is based on classic probability theory. Most of the risks that the operations of the business might be subjected to are usually known. Hence, there is usually a good idea of the cost associated with the risks. Therefore, it becomes relatively easy to calculate the level of overall risk given the following equation:

R = P × C

where R is the risk, P the probability of occurrence of an event, and C the cost if the event were to take place.

Prioritizing Decisions

The balance between strategic and operating decisions is to a large extent determined by a firm’s environment. However, there is a need to identify a broad range of objectives, both strategic and operational. Dhillon and Torkzadeh [9] undertook an extensive study of values of managers in a broad spectrum of firms. Their findings identified 25 classes of objectives for IS security. Dhillon and Torkzadeh concluded that although it is possible to classify the objectives into fundamental and means, it is rather difficult to rank them. Although tools and techniques, such as Analytical Hierarchical Modeling, are available to rank the objectives, any ranking would still be context specific. Figure 5.5 presents a network of means and fundamental objectives.

The fundamental objectives are ultimately the ones that any organization should aspire to achieve. These are also the high-level objectives that should form the basis for developing any security policy. Failure to do so will result in policies that do not necessarily relate to organizational reality. As a consequence, there is confusion in the means of achieving the security objectives. For instance, there are always calls for increasing awareness among organizational members. However, in practice there may be a lack of proper communication channels. Furthermore, responsibility and accountability structures may not exist. This results in awareness programs becoming virtually ineffective.

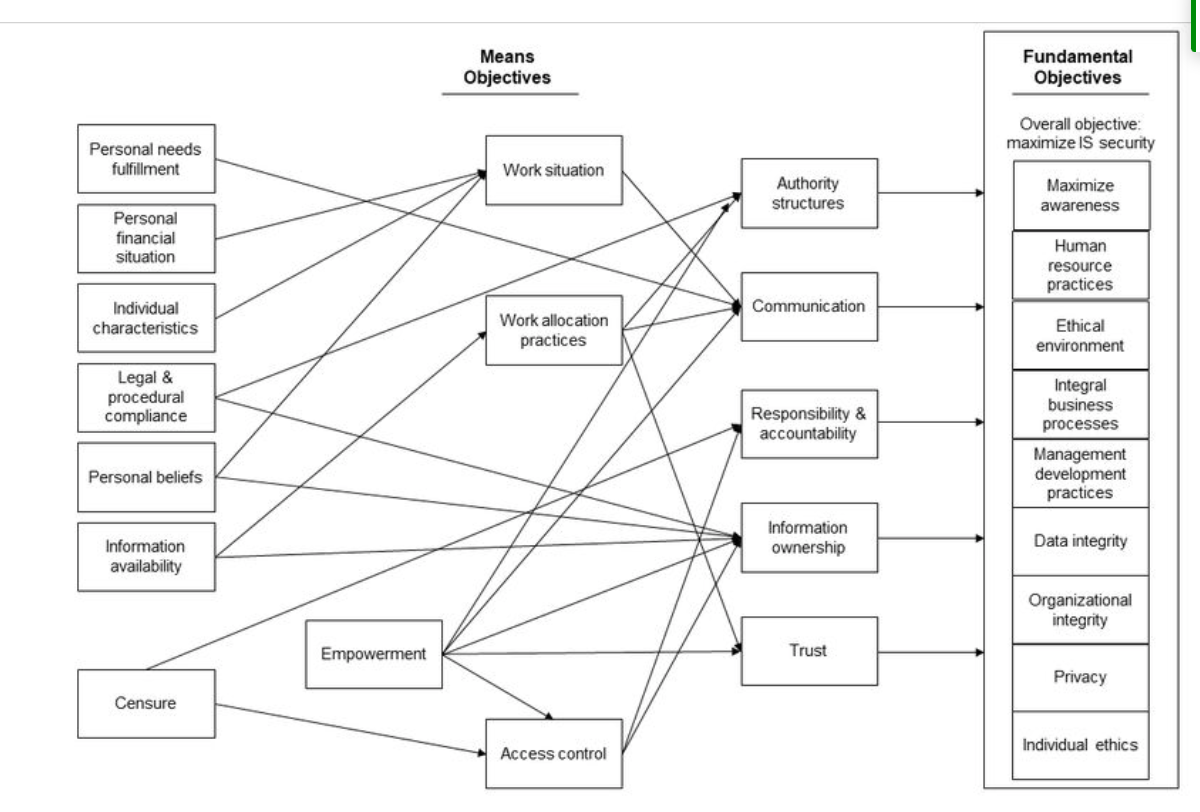


Figure 5.5. A network of IS Security means and fundamental objectives

Similarly, it may be difficult to realize any of the fundamental objectives if the appropriate means of achieving them have not been clarified. Data integrity, for example, cannot be maintained if ownership of information has not been worked out. Maintaining integrity of business processes is a function of adequate responsibility and accountability structures. Both means and fundamental objectives are a means to ensure that the espoused theory of IS security and the theory-in-use are congruent. In many ways, properly identifying and following the objectives ensures that double loop learning takes place.

Security Planning Process

The importance of planning for IS security cannot be overstated. Clearly, there is a need to systematically identify and address a range of performance gaps. Such gaps might exist in setting objectives or in establishing mechanisms for their implementation. Whatever the nature and scope of the performance gaps, there is a need to establish a method that will guide project managers, systems developers, and security analysts in ensuring that proper security is built into the organization. Usually, the primary challenge in any IS security plan is that of stakeholder involvement. This is a rather critical aspect of any security strategy. Past research has shown that a lack of understanding of what the stakeholders want is perhaps a main reason why various security policies do not get accepted in organizations.

A useful way to conceptualize security is to use Peter Checkland’s Soft System Methodology (SSM) [4]. One of the core tenets of SSM is to think of the ideal situation (systems thinking) and the real-world situation (real-world thinking). This thinking is always done by people actually involved in the work situation. In the first instance, a rich picture of the problem situation, with all its complexity, is developed. Perceptions of all stakeholders are captured. This is followed by building models of the real situation. Due consideration is given to the organizational goals and objectives. The conceptual models are then compared with the problem situation. This results in developing feasible and desirable changes that might be necessary. The various steps of SSM are used in an iterative manner. Their application is not necessarily sequential. Rather, it is important to go back to particular situations since it helps in developing clarity of an uncertain and an ambiguous situation.

SSM has been extensively used in numerous fields as a means of understanding problematic situations. Application of SSM to management of IS security has not been extensively undertaken, however. One exception is the doctoral work completed by Helen Armstrong [2] in 1999. Based on SSM Armstrong developed the Orion security strategy, which was subsequently used to manage IS security in a health care environment. The Orion model offers an alternative way to plan and manage IS security as opposed to highly structured approaches. The focus is shifted away from situations where exclusive reliance is placed on security specialists to one where users are made aware of security issues. This helps users themselves to identify a range of security controls. The result of this is that users feel responsible for IS security in their given work area. This results in developing a holistic view of security.

The situation mandated by Orion shifts the emphasis away from a security expert who might be dictating a range of protective measures. Rather, the role evolves into one of an advisor to the user and management, who feel responsible for IS security. This reduces the possibility of end user resistance to IS security mechanisms and even the implementation of inappropriate security controls. Usually, it is the end users in the organization who know of all the vulnerabilities in business processes and systems. They are also the ones who know the best methods to “plug the holes.” It, therefore, makes sense to work with the users to ensure security.

As has been discussed elsewhere in this book, traditional IS security mechanisms have largely been confined to technical and risk attributes of IS security. The Orion method is one means of shifting the focus away from an exclusively technical or a risk-dominated security approach. The method details steps to study the current and ideal security situations and identify any gaps. Appropriate measures to fill the gaps are then suggested. This allows for security to be integrated into the organizational mindset. This helps in integrating security thinking into all organizational activities rather than it being considered a separate activity.

Involving users in the Orion method has two distinct advantages:

1. It affords an opportunity to tap into the knowledge of the users. Since staff members are usually engaged in day-to-day operations, they understand the range of activities that come together to achieve a given process objective. Tapping into this knowledge domain is important since technical security experts will never be able to understand the depth of the problem situations and business processes as well as the people engaged in the activities on a day-to-day basis.

2. It also implicitly helps in increasing awareness of the range of security issues among coworkers. Since employees are involved in uncovering the security vulnerabilities and identifying protection mechanisms, they become more inclined to follow the security measures that might be implemented. As Armstrong [2] notes, “One of the keys to the success of the Orion approach is the marrying of people with information security and organizational expertise to build a holistic consciousness integrated into the organizational mindset” (p. 343).

Orion Strategy Process Overview

A high-level representation of the Orion security strategy process appears in Figure 5.6. The Orion strategy process is conceptualized at two planes of reality:

1. Level 1: This is the physical world, where all actions and processes can be seen and measured.

2. Level 2: This is the abstract or the conceptual level. Idealized processes and work situations exist at this level.

Level 2 allows participants to think beyond the confines of the physical reality and engage in creative thinking. In the Orion strategy process diagram, oval shapes denote activities. The boundary is denoted by a solid line. The boundary, usually, encompasses the main activities, separating the main area being considered. The range of inputs could include legal and regulatory requirements, policies put forward by the board of directors, inputs from other organizations/systems, etc. Outputs are the well-defined security requirements, action plans, and reporting structures. The Orion strategy process has seven steps in all. These are numbered in Figure 5.6 for reference purposes. Although it is recommended that all activities are undertaken in a sequential manner at least to begin with, following each of the steps in a “cause-effect” mode is not mandated by the process. In the remainder of this section, the details of the Orion strategy process are discussed.

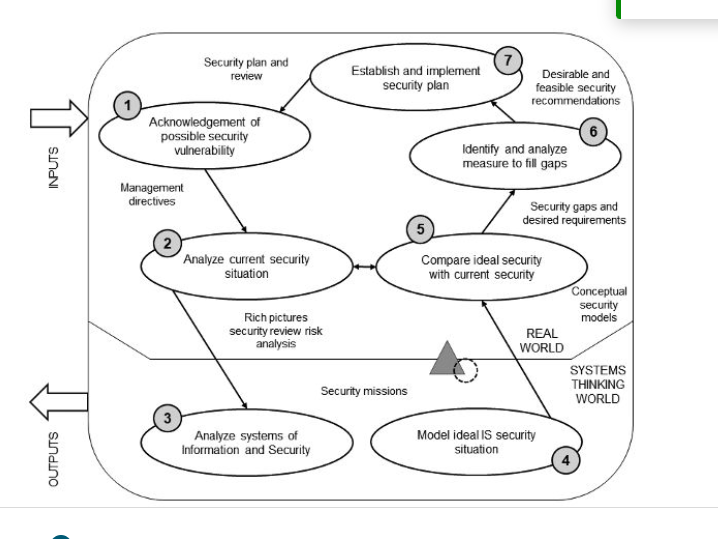


Figure 5.6. A high-level view of the Orion strategy (reproduced from Armstrong [2])

Activity 1: Acknowledgement of possible security vulnerability. This activity involves the collection of perceptions of the problem situation. Multiple stakeholders are interviewed and their perception of the situation is recorded. No analysis is undertaken per se. This not only helps in understanding the range of opinions about security, but is also a stepping stone for building consensus.

Activity 2: Identify risks and current security situation. A detailed picture of the current situation is drawn. Particular attention is given to the existing structures and processes. The structure is the physical layout of the organization, formal reporting structures, responsibilities, authority structures, formal and informal communication channels. Softer power issues are also mapped as research has shown that these do have a bearing on the management of IS security [7]. Process is looked at in terms of typical input, processing, output, and feedback mechanisms. This involves considering basic activities related to deciding to do something, doing it, monitoring the activities as progress is made, impact of external factors, and evaluating outcomes. The result of this stage is a detailed description of the situation. Usually, a lot of pictures are drawn, security reports are reviewed, and outcomes of traditional risk analysis studied.

Activity 3: Identifying the ideal security situation. At this stage hypotheses concerning the nature and scope of improvements are developed. These are then discussed with the concerned stakeholders to identify both “feasible” and “desirable” options. In particular, this involves developing a high-level definition of systems of doing things and the related security—both technical and procedural. It is important to note that a “system” should not necessarily be viewed in terms of a technical artifact. Rather, a system, as discussed in earlier parts of this book, has both formal and informal aspects. Activity 3 is rooted in the ideal world. Here we detach ourselves from the real world and think of ideal types and conceptualize ideal practices.

Activity 4: Model ideal information systems security. This stage represents the conceptual modeling step in the process. All activities necessary to achieve the agreed-upon transformation are considered and a model of the ideal security situation developed. This involves analyzing the systems of information and defining important characteristics. The security features should match the ideal types defined in Activity 3. An important step in Activity 4 is monitoring the operational system. In particular three sub-activities are undertaken:

1. Measures of performance are defined. This generally relates to assessing the efficacy (does it work), efficiency (how much work completed given consumed resources), and effectiveness (are goals being met). Other metrics besides efficacy, efficiency, and effectiveness may also be used.

2. Activities are monitored in accordance with the defined metrics.

3. Control actions are taken, where outcomes of the metrics are assessed in order to determine and execute actions.

Activity 5: Comparison of ideal with current. At this stage the conceptual models built earlier are compared with the real-world expression. The comparison at this stage may lead to multiple reiterations of activities 3 and 4. Prior to any comparison, however, it’s important to define the end point of Activity 4. There is a natural tendency to constantly engage in conceptual model building. However, it is always a good idea to move rather quickly to Activity 5 and then return to Activity 4 in an iterative manner. This not only helps in building better conceptual models, but also enables undertaking an exhaustive comparison. Comparison, as suggested in Activity 5, is an important step of the Orion strategy process. There are four particular ways in which the comparison can be done.

1. Conceptual model as a base for structured questioning. This is usually done when the real-world situation is significantly different from the one depicted in the conceptual model. The conceptual model helps in opening up a range of questions that are systematically asked to understand aspects of the real-world situation.

2. Comparing history with model prediction. In this method the sequence of events in the past are reconstructed and then comparison is done to understand what had happened in producing it and what would have happened if the relevant conceptual model was actually implemented. This helps in defining the meaning of the models, allowing for a satisfactory comparison.

3. General overall comparison. This comparison relates to discussing the “Whats” and “Hows.” The basic question addressed relates to defining features that might be different from present reality and why. In Activity 5, the comparison is undertaken alongside the expression of the problem situation expressed in Activity 2.

4. Model overlay. In this method there is a direct overlay of the two models—real world and conceptual. The differences in the two models become the source of discussions for any change.

Activity 6: Identify and analyze measures to fill gaps. This stage involves a review of the desired solution space. The wider context of the problem domain is reviewed for possible alternative solutions. The source of this review is a function of the solution that is sought. If the intent is to identify devices, then vendors are approached. If the procedures need to be redesigned, then compliance consultants need to be brought in (at least in the US where the Sarbanes-Oxley Act is mandating such compliance). It is important to note that at this stage no alternatives are dismissed. All are reviewed and adequately analyzed.

Activity 7: Establish and implement security plan. Recommendations developed in Activity 6 are considered and solutions formulated. An implementation plan is devised. Detailed tasks are identified. Criteria to subsequently measure success are also established. At this stage, integration of security into overall systems and information flows is also considered. It is important at this stage to ensure that the means used to establish security are appropriate and do not conflict with the other controls. Resources used for implementing security are then calculated and adequately allocated. Such resources would include people, skills, time, equipment, among others. On completion of implementation and training, the success is reviewed in light of the original objectives so that further learning can be achieved.

IS Security Planning Principles

It should be clear from the discussion so far that organizations need to develop a security vision that ties corporate plans with the tactical security policy issues. There are numerous cases where although information technology has been considered as a strategic resource, little effort has been made to address the security concerns. Even where security implications have been thought of, a narrow technical perspective has been considered. Such a perspective hinders progress in establishing good security. So what are the fundamental principles that organizations need to have in place if proper IS security strategies and plans are to be realized? The remaining part of this chapter discusses the principles.

Principles

In furthering our understanding of security policies, we should be able to study the security policy formulation process from the perspective of people in an organization, thus allowing us to avoid causal and mechanistic explanations. By adopting a human perspective, we tend to focus on the human behavioral aspects. Security policy formulation is therefore not a set of discrete steps rationally envisaged by the top management, but an emergent process that develops by understanding the subjective world of human experiences. Mintzberg [14] contrasts such “emergent strategies” with the conventional “deliberate strategies” by using two images of planning and crafting:

Imagine someone planning strategy. What likely springs to mind is an image of orderly thinking: a senior manager, or a group of them, sitting in an office formulating courses of action that everyone else will implement on schedule. The keynote is reason—rational control, the systematic analysis of competitors and markets, or company strengths and weaknesses, the combination of these analyses produces clear, explicit, full-blown strategies.

Now imagine someone crafting strategy. A wholly different image likely results, as different from planning as craft is from mechanization. Craft invokes traditional skill, dedication, perfection through the mastery of detail. What springs to mind is not so much thinking and reason as involvement, a feeling of intimacy and harmony with the materials at hand, developed through long experience and commitment. Formulation and implementation merge into a fluid process of learning through which creative strategies emerge. (p. 66)

This does not necessarily mean that systematic analysis has no role in the strategy process, rather the converse is true. Without any kind of an analysis, strategy formulation at the top management level is likely to be chaotic. Therefore, a proper balance between crafting and planning is needed. Figure 5.7, hence, is not a rationalist and a sequential guide to security planning, but only highlights some of the key phases in the information system security planning process. Underlying this process is a set of principles which would help analysts to develop secure environments. These are:

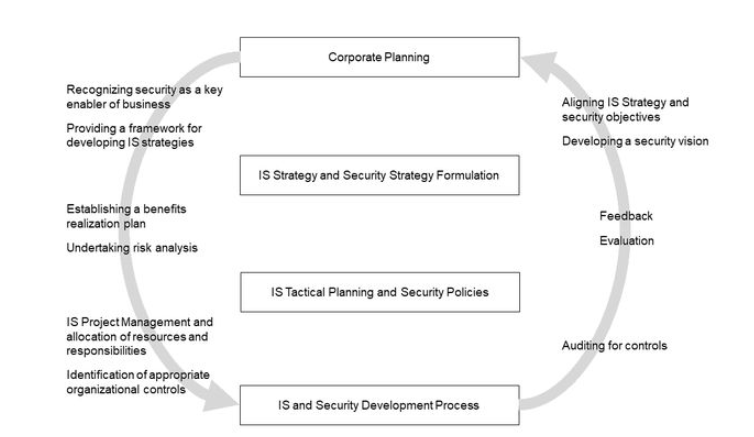


Figure 5.7. IS security planning process framework

1. A well-conceived corporate plan establishes a basis for developing a security vision. A corporate plan emerging from the experiences of those involved and the relevant analytical processes forms the basis for developing secure environments. A coherent plan should have as its objective a concern for the smooth running of the business. Typical examples of incoherence in corporate planning are seen in a number of real-life situations. The divergence of IT and business objectives in most companies and the mismatch between corporate and departmental objectives illustrate this point. Hence, an important ingredient of any corporate plan is a proper organizational and a contextual analysis. In terms of security it is worthwhile analyzing the cultural consequences of organizational actions and other IT-related changes. By conducting such a pragmatic analysis we are in a position to develop a common vision, thus maintaining the integrity of the whole edifice. Furthermore, this brings security of information systems to center stage and engenders a subculture for security.

2. A secure organization lays emphasis on the quality of its operations. A secure state cannot be achieved by considering threats and relevant countermeasures alone. Equally important is maintaining the quality and efficacy of the business operations. There is no quantitative measure for an adequate level of quality, as it is an elusive phenomenon. The definition of quality is constructed, sustained, and changed by the context in which we operate. In most companies, the attitude for maintaining the quality of business operations is extremely rationalist in nature. The management have made an implicit assumption that by adopting structured service quality assurance practices, it is possible for them to maintain the quality of the business operations. In most cases the top management assumes that their desired strategy can be passed down to the functional divisions for implementation. However, this is a very “tidy” vision of quality, whereas in reality the process is more diffuse and less structured. In fact, the “rationalist approaches” adopted by the management of many corporations causes discontentment, rancor, and alienation among different organizational groups. This is a serious security concern. A secure organization therefore has to lay emphasis on the quality of its business operations.

3. A security policy denotes specific responses to specific recurring situations and hence cannot be considered as a top-level document. To maintain the security of an enterprise, we are told that a security policy should be formulated. Furthermore, top managements are urged to provide support to such a document. However, the very notion of having such a document is problematic. Within the business management literature a policy has always been considered as a tactical device aimed at dealing with specific repeated situations. It may be unwise to elevate the position of a security policy to the level of a corporate strategy. Instead, corporate planning should recognize secure information systems as an enabler of businesses (refer to Figure 5.1). Based on this belief a security strategy should be integrated into the corporate planning process, particularly with the information systems strategy formulation. Depending on risk analysis and SWOT (strengths, weaknesses, opportunities, and threats) analysis-specific security policies should be developed. Responsibilities for such a task should be delegated to the lowest appropriate level.

4. Information systems security planning is of significance if there is a concurrent security evaluation procedure. In recent years emphasis has been placed on security audits. These serve a purpose insofar as the intention is to check deviance of specific responses for particular actions. In most cases, the whole concept of quality, performance, and security is defined in terms of conformity to auditable processes. The emphasis should be on expanding the role of security evaluation which should complement the security planning process.

Summary

The aim of this section has been to clarify misconceptions about security policies. The origins of the term are identified and a systematic position of policies with respect to strategies and corporate plans is established. Accordingly various concepts are classified into three levels: corporate, business, and functional. This categorization prevents us from giving undue importance to security policies, and allows us to stress the usefulness of corporate planning and development of a security vision. Finally, a framework for information system security planning process is introduced. Underlying the framework are a set of four principles which help in developing secure organizations. The framework considers security aspects to be as important as corporate planning and critical to the survival of an organization. An adequate consideration of security during the planning process helps analysts to maintain the quality, coherence, and integrity of the business operations. It prevents security from being considered as an afterthought.

In Brief

• Identification and development of structures of responsibility are a key aspect of formal information system security.

• Structures of responsibility define the pattern of authority, which is so essential in ensuring management of access.

• Organizational buy-in at all levels is key to the success of the information system security program in any organization.

• Security policies are an important ingredient of the overall security program.

• Proper security policy formulation and implementation is essential for the success of overall security.

• Planning for IS security entails developing a vision and a strategy for security.

• Security of IS should be thought of as an enabler to the smooth running of business.

• There are three classes of IS security decisions—strategic, administrative, and operational.

• Strategic IS security decisions deal with selecting an environment that ensures the smooth running of business.

• Administrative IS security decisions deal with creating adequate structures and processes to enable information handling.

• Operational IS security decisions relate to optimizing work patterns for efficiency gains.

• There are four core IS planning principles:

◦ A well-conceived corporate plan establishes a basis for developing a security vision.

◦ A secure organization lays emphasis on the quality of its operations.

◦ A security policy denotes specific responses to specific recurring situations and hence cannot be considered as a top-level document.

◦ IS security planning is of significance if there is a concurrent evaluation procedure.

References

1. Ansoff, H.I., Corporate strategy. 1987, Harmondsworth, UK: Penguin Books.

2. Armstrong, H., A soft approach to management of information security, in School of Public Health. 1999, Curtin University: Perth, Australia. p. 343.

3. Backhouse, J. and G. Dhillon, Structures of responsibility and security of information systems. European Journal of Information Systems, 1996. 5(1): p. 2-9.

4. Checkland, P.B. and J. Scholes, Soft systems methodology in action. 1990, Chichester: John Wiley.

5. Dhillon, G., Managing information system security. 1997, London: Macmillan.

6. Dhillon, G., The Challenge of Managing Information Security. International Journal of Information Management, 2004. 24(1): p. 3-4.

7. Dhillon, G. and J. Backhouse, Managing for secure organizations: a review of information systems security research approaches, in Key issues in information systems, D. Avison, Editor. 1997, McGraw Hill.

8. Dhillon, G. and S. Moores, Computer Crimes: theorizing about the enemy within. Computers & Security, 2001. 20(8): p. 715-723.

9. Dhillon, G. and G. Torkzadeh. Value-focused assessment of information system security in organizations. in International Conference on Information Systems. 2001. New Orleans, LA.

10. Fiol, C.M. and M.A. Lyles, Organizational learning. Academy of Management Review, 1985. 10: p. 803-813.

11. Greenwald, J., Jack in the box, in Time. 1994.

12. Greenwald, J., A blown billion, in Time. 1995. p. 60-61.

13. Mattia, A. and G. Dhillon. Applying Double Loop Learning to Interpret Implications for Information Systems Security Design. in IEEE Systems, Man & Cybernetics Conference. 2003. Washington DC.

14. Mintzberg, H., Crafting strategy. Harvard Business Review, 1987(July-August).

15. Perry, W.E., Developing a computer security and control strategy. Computers & Security, 1982. 1(1): p. 17-26

16. Ramachandran, S. and G.B. White. Methodology To Determine Security ROI. in Proceedings of the Tenth Americas Conference on Information Systems. 2004. New York, New York, August: AIS.

17. Rawnsley, J., Going for broke: Nick Leeson and the collapse of Barings Bank. 1995, London: Harper Collins.

18. Solms, B.v. and R.v. Solms, The 10 deadly sins of information security management. Computers & Security, 2004. 23: p. 371-376.

19. Wrapp, H.E., Good managers don’t make policy decisions, in The strategy process, H. Mintzberg and J.B. Quinn, Editors. 1991, Prentice-Hall: Englewood Cliffs. p. 32-38.

1 The Oxford English Dictionary defines policy as: “prudent conduct, sagacity; course or general plan of action (to be) adop