In the past decade two developments have brought information security management issues to the fore. First has been the increased dependence of organizations on information and communication technologies, not only for key operational purposes but also for gaining strategic advantage. Second, abetted by information and communication technologies, the whole business model for many organizations has been transformed. Whereas in the past companies could rely on confining themselves to a particular geographical area to conduct their business. Today companies are increasingly becoming location independent and are finding themselves to be strategically disadvantaged if they are confined to a particular place. The consequence of advances in information technologies and the changing boundaries of the firm have brought the importance of data and information to the fore. This is because it is information that helps companies realize their objectives and helps managers to take adequate decisions. In the business model of the past, data and information to a large extent was confined to a particular location and it was relatively easy to protect it from falling in the hands of those who should not have it (i.e. maintain confidentiality). Because information was usually processed in a central location, it was also possible to ensure, with a relative degree of certainty, that it’s content and form did not change (i.e. maintain integrity) and ensure that it was readily accessible to authorized personnel (i.e. maintain availability). In fact maintaining confidentiality, integrity and availability were the main tenants for managing security. Today because the nature of the organization and scope of information processing has evolved, managing information security is not just restricted to maintaining confidentiality, integrity and availability. Perhaps as Dhillon and Backhouse (2000) point out, the emphasis should be on establishing responsibility, integrity of people, trustworthiness and ethicality.

Changing structures, advances in information and communication technologies and the greater reliance of companies on information indeed poses a number of challenges for maintaining good management practices. In recent years clearly organizations have fallen short of developing adequate policies to deal with the information security problems. Various authors have reported increases in incidents of computer crimes because of violation of safeguards by internal employees of organizations (as high as 80% of total computer crimes – e.g. see Dhillon (1999a). There also seems to be a ‘policy vacuum’ to deal with information security problems. This is evidenced not only by increases in incidents of system penetration (e.g. hacking), but also in inability of authorities to
establish adequate basis to deal with such computer crimes. One example is the case of Randal Shwartz where there were difficulties to establish whether illicit use of computers by Shawartz amounted to an occurrence of a computer crime (Dhillon, 2000). Advances in information technologies have introduced a yet another kind of a problem for organizations, which many classify as ‘input crimes’ (Dhillon, 1999b). In one case a former employee of a wholesaler was convicted under the UK Computer Misuse Act when he obtained for himself a 70% discount when the regular staff of the wholesaler were otherwise engaged. Given the increased dependence of businesses on computers, one would assume that most companies would have well established contingency and disaster recovery plans. Unfortunately research seems to suggest otherwise. Based on survey findings Adam and Haslam (2001) suggest that adequate importance is not being placed on disaster recovery planning. Many managers tend to think that disaster recovery planning is an insignificant issue and hence prefer to concentrate on projects that generate revenues.

THE CHALLENGES

It goes without saying that, incidents of computer crime, information security problems and information technology enabled frauds have been on the increase. And any attempt to deal with the problem demands an adequate understanding of the challenges that exist in the new millennium. Such challenges can be classified into four categories:

- The challenge of establishing good management practices in a geographically dispersed environment and yet being able to control organizational operations.
- The challenge of establishing security policies and procedures that adequately reflect the organizational context and new business processes.
- The challenge of establishing correct structures of responsibility, given the complex structuring of organizations and information processing activities.
- The challenge of establishing appropriate information technology disaster recovery plans.

Numerous studies have indicated that there is a problem in managing information security especially with respect to regulating the behavior of internal employees. Research has also shown that many a times internal employees subvert existing controls to gain undue advantage essentially because either an opportunity exists to do so or they are disgruntled (Backhouse and Dhillon, 1995). The problem gets compounded even further when an organization is geographically dispersed and it becomes difficult to institute the necessary formal controls. This was evidenced in the case of Nick Leeson who brought about the downfall of Barings Bank in Singapore. Barings collapsed because by relying on information technology Leeson was able to successfully conceal the positions and losses from the Barings management, internal and external auditors, and regulatory bodies in Singapore and the Bank of England. Leeson’s case is illustrative of breaches of control, trust, confidence, and deviations from conventional accounting methods or expectations.

The management of Barings had confessed in one of the internal memos that clearly their systems and controls were distinctly flaky. However there was nothing new in this
confession, since it has long been established that lapses in applying internal and external controls is perhaps the primary reason for breaches in information security (see Audit Commission, 1990; 1994). Failure of management to curtail Leeson's sole responsibilities, which empowered him to create an environment conducive to crime, lack of independent monitoring and control of risk, communication breakdown between managers, and the belief that information technology can overcome basic communication problems in organizations were other reason that created an opportunity for Lesson to engage in a criminal act.

There is also the challenge of establishing appropriate security policies and procedures that adequately reflect the organizational context and new business processes. Such challenges exist at two levels. First at an internal organizational level where it is increasingly becoming difficult for businesses to develop and implement appropriate security policies. Second at a broad contextual level, where it is becoming difficult to rely on traditional legal policies to regulate behavior. At an internal organizational level, there is a problem with respect to establishing security policies. For one there is a lack of awareness within organizations that such a need exists. Based on a longitudinal study of information security problems within the health services sector and the local government councils, Dhillon (1997) contends that there is not only a lack of commitment from top management in the security policy formulation process, but security policies are conceived in a formal-rational manner. This results in an ‘acontextual’ assessment of the security problems and the responses address the issues in a rather superficial manner.

At a broad contextual level, although a number of cyberlaws have been enacted in recent years their nature and scope seems to be at odds with the reality. Clearly there are a number of computer crime situations where it is important to institute punitive social controls in order to curtail criminal activities, and in some cases to recover stolen money or goods. There are perhaps a number of other computer crimes where severe punitive control may not be the best option. In many cases monetary gain is not the prime motive, the intellectual challenge of tearing apart computer systems is. In such cases it would perhaps be counter-productive to institute severe punitive controls.

Another challenge in managing information system security in the new millennium relates to establishing correct structures of responsibility. Information security problems resulting from either the inability to understand the nature and scope of such structures within organizations or to specify new ones are abound. When Japan’s Daiwa Bank fell short of understanding the patterns of behavior expected of businesses operating out of the US and allowed Japanese normative structures to dominate, it resulted in a bond trader, Toshihide Iguchi, accruing losses to the tune of $1.1 billion. Besides it also allowed Iguchi to engage in at least 30,000 illicit trades. The drama ended in Iguchi being prosecuted and Daiwa’s charter to conduct business in the US being suspended. Situations such as the one represented by Daiwa pose a challenging issue of managing access to information processing facilities. Merely stating ‘read only’ or ‘write only’ accesses matching an organization’s hierarchical structure are insufficient, especially in light of the changing organizational forms. Dhillon and Orton (2000) have argued that modern enterprises are in a constant state of ‘schizoid incoherence’ and there are very short spells of stability in organizational forms. This is especially true for businesses that tend to organize themselves in a ‘networked’ or ‘virtual’ manner. The evolving
organizational forms seem to question the applicability of formal methods in instituting access control.

It is indeed a challenge when dealing with information technology disaster recovery plans and policies. Many a times disasters occur because of complacency of staff. Recently Northwest Airlines were left to wonder why their backup system was disabled. In fact a sub-contractor laying new lines in Eagan, Minnesota bored through a cluster of cables and ended up cutting 244 fiber optic and copper telecommunications lines. As a consequence airline passengers nationwide were left stranded since the lines linked the Northwest’s Minneapolis-St. Paul hub to the rest of the nation. Apparently the redundant system lines ran alongside the ones used for backing up (Lehman, 2000). A 1996 IBM survey on business continuity practices, “A risk too far”, reported that the 300 companies surveyed had suffered 293 events in 1995 alone. The loss of system capability was estimated to have threatened some 500,000 manhours of work in the respective locations. The IBM study suggested that 89% of the companies surveyed believed their PCs to be critical. Nearly a quarter of the companies stored 60% of their data on the PCs and 76% were not aware of the cost of back up. Over the years the situation has not changed.

SEARCHING FOR A SOLUTION

Solutions to the problem of managing information security in the new millennium hark back at shifting emphasis from technology to business and social process. Although many researchers have placed calls for such an orientation, in practice over-formalized, acontextual and ahistorical solutions designed in a reactive manner, still dominate. Many a times such ill-conceived solutions mark the beginning of a disastrous information technology implementation with an inadequate consideration of information security.

Establishing formalized rules is one step that could lead towards a solution for managing information security. Such formalized rules may take the form of security policies that help in facilitating bureaucratic functions in order to resolve ambiguities and misunderstandings within organizations. Both academics and practitioners have made numerous calls for formulating security policies and many of these calls have stopped at just that. Although security policies are essential for laying down rules of conduct, success of security policies is clearly a function of the level of their integration with the strategic vision. If we accept that a secure environment is an enabling condition for the smooth running of an enterprise, then security considerations are a strategic issue and there is a need to configure them for maintaining the consistency and coherence of organizational operations.

In the past security policies have been formulated based on checklists and hence tend to identify specific responses to specific conditions. However if organizations want information security management to be an antecedent to a highly integral business environment, focus needs to shift towards creating a security vision and strategy where adequate consideration is given to the threats and weaknesses of the information technology infrastructure within the broader scope of computerization. Security policies then tend to take on the role of functional strategies. This not only moves the information security agenda to the top management list, but also ensures buy in from the senior management stakeholders. Arguments in support of formulating an information security vision and strategy stem from the corporate strategy literature where it has been
contended that “good managers don’t make policy decisions” (Wrapp, 1991; p32). By focusing on a security vision instead the danger of being trapped in arbitrating disputes arising from a stated policy are elevated. A detailed discussion focusing on the importance of a security vision appears in Dhillon (1997) pg 137-142.

Hitchings (1994) has suggested the importance of considering human issues in designing information security and uses a ‘virtual methodology’ to consider human centered controls in an organization and its environment (Hitchings, 1996). Clearly a lack of human centered controls result in increasing the probability of occurrence of adverse events. Such events could either be a consequence of disgruntled employees or merely an opportunity being exploited. Poor quality of management and inadequate management communication has also been considered as precursors of an unethical environment, thus making an organization vulnerable to a crime. Since most organizational workplaces are characterized by such predicaments, the importance of establishing an ethical environment within an organization cannot be overstated.

In proposing solutions to information security problems arising because of inability to appreciate human factors, Dhillon (1999a) calls for establishing normative controls. Normative controls are a byproduct of a dominant security culture, which is the totality of patterns of behavior in an organization that contribute to the protection of information of all kinds. A lack of a security culture results in problems of maintaining integrity of the whole organization and indirectly threatens the protection of technical systems. Most adverse events can be traced back to a lack of security culture and a consequence of breakdown in organizational communications. An issue related to the security culture is that of monitoring employee behavior. As Backhouse and Dhillon (1995) note, besides personal factors, work situations and opportunities available allow individuals to perform criminal acts. Evidence to this contention appears in Dhillon (1999a), where its shown that the prevalent work situation and the opportunity to commit criminal acts at Kidder Peabody affected the primary belief system of perpetrator, thus resulting in a criminal act being performed. The ability to leverage work situations and opportunities to engage in computer crimes suggests that monitoring of employee behavior is an essential step in maintaining the integrity of an organization. Such monitoring does not necessarily have to be formal and rule based. In fact informal monitoring, such as interpreting behavioral changes and identifying personal and group conflicts, can help in establishing adequate checks and balances.

In the previous section the problems with establishing structures or responsibility was mentioned. 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. Backhouse and Dhillon (1996) introduced the concept of structures of responsibility to the information security literature. And suggest that such structures provide a means to understand the manner in which responsible agents are identified within the context of the formal and informal organizational environments. A ‘structures of responsibility’ focus also facilitate an understanding of the range of conduct open to the responsible agents, the influences they are subjected to, the manner in which they signify the
occurrence of events, the communications they enter into. The most important element of interpreting structures of responsibility is the ability to understand the underlying patterns of behavior. The positive connotations of interpreting behavioral attributes in developing and designing secure environments has been well documented (e.g. refer to the studies conducted by Dhillon and Backhouse, 1997; Dhillon, 1997; Dhillon, 1999a; Dobson, 1991).

Besides focusing on formalized rule structures and establishing an adequate understanding of behavioral practices, it is also important to develop and implement adequate technological controls. Adequacy and appropriateness are a key to the design of technical control measures. In the literature there are a number of approaches available. And most of these have been tested for their validity and completeness. The US Department of Defense has been using the Trusted Computer System Evaluation Criteria for years, and clearly they are valid and complete. So are the Bell La Padula and Denning Models for confidentiality of access control. Similarly the validity and completeness of other models such as Rushby’s Separation Model and Biba Model for integrity has also been established. However their validity exists not because of the completeness of their internal working and their derivations through axioms, but because the reality they are modeling is well defined, i.e. the military organization. The military, to a large extent, represents a culture of trust among its members and a system of clear roles and responsibilities. Hence the classification of information security within the models does not represent the constructs of the models, but instead reflect the very organization they are modeling. A challenge, however, exist when business organizations are using models based on a different reality. Obviously in the commercial environment the formal models for managing information security fall short of maintaining their completeness and validity.

PRINCIPLES FOR MANAGING INFORMATION SECURITY

Previous sections have focused on identifying problems and challenges in managing information security in various contexts. The focus of this section is to present a synthesized framework for managing information security in the electronic years. It is important to develop such a conceptual understanding since the challenges of managing information security permeate various aspects of our personal and business life. May it be booking flights over the Internet, buying a book or simply browsing to gather information, challenges to protect personal information exist and there are simply no straightforward answers. Similarly for businesses, protection of information is absolutely critical. Obviously no company would like, for example, its competitors to have access to their sales data. Or for that matter, companies would neither appreciate unauthorized use of computers by their employees nor would a violation of safeguards by trusted personnel go down very well. For these reasons it is important that companies consider certain fundamental principles that could be used as pointers for not only establishing an information security vision and strategy, but would also facilitate in mapping out a detailed security policy.

This chapter sketches out three classes of principles. Following a brief description of the class, each principle is elaborated and suggestions made thereof as to its applicability. The three classes of principles are:

- Principles for managing the pragmatic aspects of an organization.
• Principles for managing the formal rule based aspects of an organization
• Principles for managing the technical systems

PRINCIPLES FOR MANAGING THE PRAGMATIC ASPECTS

Clearly the importance of broader social and organizational issues in managing information security concerns cannot be underestimated. Pouloudi (2001) argues that a particular context may make fraud a legitimate activity. Therefore it is important to understand the context in which an information technology is being implemented. She further suggests that by carefully interpreting issues and concerns of various stakeholders, it is possible to understand the interaction between technical and social aspects of an information technology implementation, thus facilitating fraud prevention. Research done by Dhillon and Backhouse (1996) is also in a similar vein. By evaluating the unethical computer use practices of Jett at Kidder Peabody, it is suggested that it is important to inculcate a culture or trust and responsibility. It becomes apparent therefore that organizations need to develop a focus on the pragmatic aspects in managing information system security. The various principles that need to be adopted are as follows.

Principle 1: Education, training and awareness, although important, are not sufficient conditions for managing information security. A focus on developing a security culture goes a long way in developing and sustaining a secure environment.

Research has shown that although education, training and awareness are important in managing the security of enterprises, unless or until an effort to inculcate a security culture exists, complete organizational integrity will be a far-fetched idea. Dhillon (1997) has suggested that “a mismatch between the needs and goals of the organization could potentially be detrimental to the health of an organization and to the information systems in place…. organizational processes such as communications, decision making, change and power are culturally ingrained and failure to comprehend these could lead to problems in the security of information systems” pg 111. While discussing issues in disaster recovery planning, Adam and Haslam (2001) notes that although managers are aware of the potential problems related with a disaster, they tend to be rather complacent in taking any proactive steps. Such an attitude could be a consequence of the relative degree of importance placed on revenue generation. As a consequence, while automating business processes and in a quest for optimal solutions, back-up and recovery issues are often over looked.

Principle 2: Responsibility, integrity, trust and ethicality are the cornerstones for maintaining a secure environment. Earlier on we noted that given that the nature of organizations has evolved from a predominantly hierarchical organization to a more networked form, traditional security models and approaches fall short of developing secure environments. Dhillon and Backhouse (2000) have argued that traditional “information security principles of Confidentiality, Integrity and Availability are fine as far as they go, but they are very restricted”. In response to the changing organizational contexts they suggest the RITE (responsibility, integrity, trust and ethicality) principles. The RITE principles hark back to an earlier time period when extensive reliance on technology for close supervision and control of dispersed activities was virtually non-existent. Beniger (1986) terms this as the ‘factorage system of distributed control’ where the trade between cotton producers in America and British merchants was to a large
extent based on trust (pg 132-133). The extensive reliance on information technologies today questions the nature and scope of individual responsibilities and many a times challenges the integrity of individuals. Trust is also broken especially when technology is considered as an alternative supervisor.

PRINCIPLES FOR MANAGING THE FORMAL RULE BASED ASPECTS

Research conducted by organizational theorists has suggested that formalized structures are a consequence of increased complexity within organizations. Mintzberg (1983) illustrates this assertion by narrating Ms Raku’s story of her pottery business and how she organized her work as her business evolved from a basement shop to Ceramics Inc. (pg 1). Computers are subsequently used to automate many of the formal activities in a business. And there is always a challenge in deciding as to which aspects one should computerize and which should be left alone (for a detailed description see Liebenau and Backhouse, 1990; pg 62-63). It is important therefore to understand the nature and scope of formal rule based systems and understand as to how information security could be adequately designed into an organization. The following paragraphs present principles that need to be considered in instituting adequate control measures.

Principle 3: Establishing a boundary between what can be formalized and what should be norm based is the basis for establishing appropriate control measures. Clearly security problems arise as a consequence of ‘over-formalization’ and managerial inability to balance the rule and norm based aspects of work (see arguments presented in Dhillon, 1997; pg 157-160). At a formal level an organization needs structures which support the technical infrastructure. Therefore formal rules and procedures need to be established which support the IT systems. This would prevent the misinterpretation of data and misapplication of rules, thus avoiding potential information security problems. In practice, however, controls have dysfunctional effects. This is primarily because isolated solutions (i.e. controls) are proposed for specific problems. These ‘solutions’ tend to ignore other existing controls and their contexts.

Principle 4: Rules for managing information security have little relevance unless they are contextualized. Following on from the previous principle, exclusive reliance on either the rules or norms falls short of providing adequate protection. Clearly an inability to appreciate the context while applying rules for managing information security is perhaps detrimental to the security of an enterprise. It is therefore important that a through review of technical, formal and pragmatic interventions is conducted. Many a times a security policy is used as a vehicle to create a shared vision to assess how the various controls will be used and how data and information will be protected in an organization. Typically a security policy is formulated based on sound business judgment, value ascribed to the data and related risks associated with the data. Since each organization is different, the choice of various elements in a security policy is case specific and it’s hard to draw any generalization.

PRINCIPLES FOR MANAGING THE TECHNICAL SYSTEMS

With the discussion presented in this and the previous chapters, it would have become apparent that security of the technical edifice is clearly a function of the level of assurance provided by the formal and pragmatic organizational arrangements. This is
because organizations are usually viewed as purposeful systems and security has traditionally not been considered part of the ‘useful system’ designed for the purposeful activities (Longley, 1991; p 707). Rather security has always been considered as a form of guaranty that the useful activities of an organization will continue to be performed and any untoward incidents prevented. Dhillon (1997) however, in his previous work, challenges this mindset and calls for developing security visions and strategies, where information security management is considered a key enabler in the smooth running of an enterprise. Two fundamental principles need to be considered for adequately managing the technical systems. These are presented below.

**Principle 5: In managing the security of technical systems a rationally planned grandiose strategy will fall short of achieving the purpose.** There has been an ongoing debate between those who support rationally planned strategies and those who consider strategy formulation and implementation as an emergent phenomenon. There are others who have suggested that a context is the determining factor in ones choice of a rationally planned or an emergent strategy. Within the domain of information technology management, characterized by emergence of new technologies, constant innovation and its unique influence of structure and management processes, context seems to have a profound influence on maintaining organizational integrity. In recent years, the context has become even more important since newer technologies have constantly been redefining the boundaries of the firm. In an earlier era, when a hierarchy was the dominant organizational structure, a rationally planned approach for information security development and implementation would have sufficed. However with the emergence of networked and virtual enterprises, a rationally planned grandiose strategy would perhaps fall short of achieving the purpose, i.e. managing the security of technical systems.

**Principle 6: Formal models for maintaining the confidentiality, integrity and availability (CIA) of information cannot be applied to commercial organizations on a grand scale. Micro-management for achieving CIA is the way forward.** Any formal model is an abstraction of reality. The preciseness of a model is judged on basis of the extent to which it represents a given subset of the reality. Most information security models were developed for the military domain and to a large extent are successful in mapping that reality. It is possible to do so since the stated security policy is precise and strictly adhered to. In that sense a security model is a representation of the security policy rather than the actual reality. This suffices as far as the organization works according to the stated policy. In recent years however, with the widespread reliance on Internet to conduct business, problems arise at two levels. First, the organizational reality is not the same for all enterprises. This means that the stated security policy for one organization is bound to be different from that of the other. Second, a model developed for information security within a military organization may not necessarily be valid and true for a commercial enterprise. It follows therefore that any attempt to use models based on the military, are bound to be inadequate for the commercial organizations. Rather, their application in a commercial setting is going to generate a false sense of security (This assertion is based on a definition of security that goes beyond simple access control methods. For a detailed discussion of information security definitions see Dhillon (1997). The way forward is to create newer models for particular aspects of the business for which information security needs to be designed. This would mean that micro-strategies be created for unit or functional levels.
CONCLUSION
This chapter has presented six principles for managing information security in the new millennium. Information security has always remained an elusive phenomenon and it is rather difficult to come to grips with it. No one approach is adequate in managing the security of an enterprise and clearly a more holistic approach is needed. The chapter has addressed a number of diverse topics. These have ranged from security policies and ethics to computer fraud and crime. These will indeed go a long way in helping research and practice.

REFERENCES
Dhillon, G., "Managing and controlling computer misuse," Information Management & Computer Security, Volume 7, Number 5, 1999b,
Dhillon, G., "Analyzing myth and reality of computer crimes," Proceedings of the BITWorld Conference, Mexico City, Mexico, 2000,


