

Chapter I

Challenges in Managing Information Security in the New Millennium

Gurpreet Dhillon
College of Business, University of Nevada, Las Vegas

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 its 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 & 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 and Phukan, 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 & 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 (for a summary and review see Mikko Siponen’s chapter in this book, besides Dhillon et al, 1996; Dhillon, 1997) 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 & 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 believe that information technology can overcome basic communication problems in organizations were other reason that created an opportunity for Leeson 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. The importance for developing a security policy is also identified by Whitman et al in their contribution for this book.

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 & 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. Adam & Haslam's (2001) study of Irish experiences in disaster recovery planning, appearing in this book, presents a similar scenario.

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 by product 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 & 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 it is 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 & 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 & 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.

ORGANIZATION OF THE BOOK

The book is organized into twelve chapters. A brief description of each of the chapters follows:

Chapter 1 identifies the existing challenges in the management of information security in the new millennium. The chapter sets the scene for discussions presented by various authors. In particular the chapter identifies the global orientation of businesses and the related problems with managing information security. It also identifies the importance of establishing security policies, structures of responsibility and disaster recovery plans.

Chapter 2 establishes the need for a security policy and presents a sample structure that may be used to develop such a policy. The authors of this chapter contend that by investing in the development of a security policy, a business organization ensures the highest level of protection against all sorts of threats.

Chapter 3 takes philosophical orientation and debates about the rights and wrongs in the information age. The author examines some challenges in ethical management of information technology resources. The overall aim of the chapter is to consider moral issues pertaining to computer use and misuse and articulate methods of thinking through various concerns.

Chapter 4 reviews the ethical elements of security such that trust could be promoted in electronic commerce. The authors argue that trust raises confidence and hence business reputation, which is so important when engaging in online transactions. They further suggest that importance be paid to developing ethical policies.

Chapter 5 reviews the information security threats posed by international terrorist organizations. The authors classify the competence of terrorist outfits to engage in cyber-terrorism into 6 levels and identify the increased vulnerability of the information and communication networks.

Chapter 6 presents an analysis of issues and concerns in managing computer-related fraud. The authors ground their arguments in the British National Health Services and address the issue of prescription fraud. The author contends that in order to manage computer-related frauds, one needs to consider technological 'solutions' in their broader context and assess the impact of social and political factors on a business process.

Chapter 7 addresses the issue of disaster recovery planning, with particular reference to Ireland. Based on a survey, the authors suggest that there seems

to be reluctance on part of the organizations to fully commit to the provisions of a workable disaster recovery plan. In most cases although there may be a few elements of the plan in place, little emphasis has been placed on drawing them together into a coherent policy.

Chapter 8 analyses and compares recent approaches for development of secure information systems. The author systematically reviews the philosophical assumptions and presents gaps and problems in each of the current approaches. A systematic position for future research and practice is then established.

Chapter 9 reviews issues surrounding e-business security. The authors argue that it is possible to maintain Internet security and hence facilitate e-businesses, if adequate importance is placed on technical security measures. The authors present an array of technical tools and techniques that help in achieving this purpose.

Chapter 10 discusses generic concepts of compliance monitoring for anomaly detection systems. The author contends that with the emergence of electronic commerce, focus on security and compliance issues is important, if integrity of business transactions is to be maintained.

Chapter 11 presents the notion of 'intelligent agents', which is a technical means to information handling. The authors, following their identification of various security concerns, identify the role agent technology can play in security management.

Chapter 12 concludes and presents principles necessary for managing information security in the new millennium. The principles are classified into three categories, - pragmatic, formal and technical.

REFERENCES

- Adam, F., & Haslam, J. A. (2001). A study of the Irish experience with disaster recovery planning: high levels of awareness may not suffice. In G. Dhillon (Ed.), *Information security management: global challenges in the next millennium*. Hershey, PA: Idea Group Publishing.
- Audit Commission. (1990). *Survey of computer fraud & abuse*: The Audit Commission for Local Authorities and the National Health Service in England and Wales.
- Audit Commission. (1994). *Opportunity makes a thief. Analysis of computer abuse*: The Audit Commission for Local Authorities and the National Health Service in England and Wales.
- Backhouse, J., & Dhillon, G. (1995). Managing computer crime: a research outlook. *Computers & Security*, 14(7), 645-651.
- Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, 5(1), 2-9.
- Dhillon, G. (1997). *Managing information system security*. London: Macmillan.
- Dhillon, G. (1999a). Computer crime: interpreting violation of safeguards by trusted personnel. In M. Khosrowpour (Ed.), *Managing information technology*

- resources in organizations in the next millennium* (pp. 602-606). Hershey: Idea Group Publishing.
- Dhillon, G. (1999b). Managing and controlling computer misuse. *Information Management & Computer Security*, 7(5).
- Dhillon, G., & Phukan, S. (2000). *Analyzing myth and reality of computer crimes*. Paper presented at the BITWorld Conference, Mexico City, Mexico.
- Dhillon, G., & Backhouse, J. (1997). Managing for secure organizations: a review of information systems security research approaches. In D. Avison (Ed.), *Key issues in information systems* : McGraw Hill.
- Dhillon, G., & Backhouse, J. (2000). Information system security management in the next millennium. *Communications of the ACM*, 43(7).
- Dhillon, G., & Orton, J. D. (2000). *Schizoid incoherence and strategic management of new organizational forms*. Paper presented at the International Academy of Business Disciplines, March 30-April 2, Las Vegas.
- Dhillon, G., Silva, L., & Backhouse, J. (1996). *Computer crime at CEFORMA: a case study*. Paper presented at the ETHICOMP 96, Madrid, Spain, November.
- Dobson, J. (1991). A methodology for analyzing human and computer-related issues in secure systems. In K. Dittrich, S. Rautakivi, & J. Saari (Eds.), *Computer security and information integrity* (pp. 151-170). Amsterdam: Elsevier Science Publishers.
- Hitchings, J. (1994). *The need for a new approach to information security*. Paper presented at the 10th International Conference on Information Security (IFIP Sec '94), 23-27 May, Curacao, NA.
- Hitchings, J. (1996). A practical solution to the complex human issues of information security design. In S. K. Katsikas & D. Gritzalis (Eds.), *Information systems security: facing the information society of the 21st century* (pp. 3-12). London: Chapman & Hall.
- Lehman, D. (2000). Cable cuts ground Northwest flights. *Computer World*.
- Wrapp, H. E. (1991). Good managers don't make policy decisions. In H. Mintzberg & J. B. Quinn (Eds.), *The strategy process* (Second ed., pp. 32-38). Englewood Cliffs: Prentice-Hall.