

**Coping with Systems Risk:  
Security Planning Models  
for Management Decision-Making**

**Detmar W. Straub**

**Richard J. Welke**

**Working paper  
Georgia State University**

**Published as:** Straub, D.W. and Welke, R.J. "Coping with Systems Risk: Security Planning Models for Management Decision-Making," *MIS Quarterly* (22:4, December), 1998, pp. 441-469.

Please address all correspondence to:

**Detmar W. Straub  
Department of Computer Information Systems  
College of Business Administration  
Georgia State University  
Atlanta, GA 30302-4015  
dstraub@gsu.edu  
(404) 651-3827  
FAX: (404) 651-3842**

**Copyright © Detmar W. Straub and Richard J. Welke, 1996, 1998  
All rights reserved.**

# Coping with Systems Risk: Security Planning Models for Management Decision-Making

## ABSTRACT

The likelihood that the firm's information systems are insufficiently protected against certain kinds of damage or loss is known as "systems risk." Risk can be *managed* or *reduced* when managers are aware of the full range of controls available and implement the most effective controls. Unfortunately, they often lack this knowledge and their subsequent actions to cope with systems risk are less effective than they might otherwise be. This is one viable explanation for why losses from computer abuse and computer disasters today are uncomfortably large and still so potentially devastating after many years of attempting to deal with the problem. Results of comparative qualitative studies in two information services Fortune 500 firms identify an approach that can effectively deal with the problem. This theory-based security program includes: (1) use of a security risk planning model, (2) education/training in security awareness, and (3) Countermeasure Matrix analysis.

## **Introduction**

The likelihood that a firm's information systems are insufficiently protected against certain kinds of damage or loss is known as "systems risk." The underlying problem with systems risk is that managers are generally unaware of the full range of actions that they can take to reduce risk. Because of this lack of knowledge, subsequent actions to plan for and cope with systems risk are less effective than they need be. This is one viable explanation for why losses from computer abuse and computer disasters today are still so uncomfortably large and potentially devastating.

Fortunately, there are well established behavioral theories and other conceptual models that offer insight into how managers can cope with systems risk. First, general deterrence theory posits generic actions that directly and indirectly lower systems risk, exemplified, in the systems arena, by actions taken by computer security officers (Straub, 1990). Second, Simon's (1980) model of managerial decision-making offers direction as to generic stages in an effective planning approach.

An agenda for management action is proposed to deal with the problem. Managers should initiate a theory-based security program that includes: (1) use of a security risk planning model, (2) education in security awareness, and (3) Countermeasure Matrix analysis. The viability of the approach is validated through qualitative studies in two information services Fortune 500 firms.

## **Threats to Organizational Information Resources**

Information security continues to be ignored by top managers, middle managers, and employees alike. The result of this unfortunate neglect is that organizational systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary. The underlying problem is that many managers are not well versed on the nature of systems risk, likely leading to inadequately protected systems.

Organizational information systems today remain in jeopardy. Over the years study after study has documented actual and potential systems losses (Parker, 1976; 1981; 1983; Hoffer and Straub, 1989; Loch, Carr, and Warkentin, 1992). A partial listing of institutional sponsors of high profile studies includes: the U.S. Government (Kusserow, 1983; Colton, Tien., Davis, Dunn and Barnett (1982a, 1982b), the American Bar Association (1984), the American Institute of Certified Public Accountants (1984), Ernst and Young (Burger, 1993), and Ernst & Young (Panettieri, 1995), and,

abroad, the Local Government Audit Inspectorate (1981). Estimates of annual losses vary, but some set losses at between \$500 million and \$5 billion per year in the U.S. alone (Flanagan and McMEnamin, 1992). If anything, losses have become even more serious as time goes on (Schwartz, 1990).

### **Back-Burner Issue**

Yet, in spite of voluminous public evidence that systems risk is high and that many organizations are under-secured, many managers continue to ignore the issue and to be "naive" in their responses to the challenge posed by this growing threat (Loch et al., 1992, p. 183). Why is this so? One viable explanation is that systems risk has been a back-burner issue for decades, even among managers who specialize in information technology (IT), and it is difficult to change a perception with such momentum. Tellingly, although IT executives have included systems security in their list of critical issues (Ball and Harris, 1982; Dickson et al., 1984; Hartlog and Herbert, 1986; Brancheau and Wetherbe, 1987; Niederman, Brancheau, and Wetherbe, 1991), only once have they ranked it among the top ten issues. Even more tellingly, both "disaster recovery" and "security and control" dropped off the top twenty ranking in the latest key issues study (Brancheau, Janz, and Wetherbe, 1996).

### **The Nature and Extent of Systems Risk**

Assuming that there is reason to be concerned, how should prudent managers begin to think about systems risk? Risk is the uncertainty inherent in doing business; technically, it is the probability associated with losses (or failure) of a system multiplied by the dollar loss if the risk is realized. The concept of risk applies to a wide range of systems, from physical systems for delivering goods/services to a customer to computer-based systems for delivering information. The former risks are *business risks*; the latter, *systems risks*. Systems losses and failures are broadly construed to mean modification, destruction, theft, or lack of availability of computer assets such as hardware, software, data, and services. It would, thus, include computer abuse, disaster scenarios, violations of intellectual property resident in computer systems, etc.

Systems security risk — the risk that the firm's information and/or information systems are not sufficiently protected against certain kinds of damage or loss — is one form of systems risk. Another is

project risk, the risk that a systems development project will fail (Keil, 1995). In either case, to assess overall risk, one needs to have some idea about the probability of suffering losses and the extent of loss.

Systems risks vary, but one useful division is that between the risk of a *disaster* and the risk of a *computer abuse*. In all likelihood, the most serious risk confronting an organization is that mission-critical information systems will become unavailable to process the company's basic transactions. The nightmare scenario for this is the "disaster" or "catastrophe" (Peach, 1991) — events such as hurricane, earthquake, fire, or sabotage.

The risk of catastrophic loss of the organization's systems notwithstanding, managers should consider the threat from unauthorized and/or illicit penetration of the firm's computers, that is, computer abuse, with equal concern (Hoffer and Straub, 1989). Bad actors who exploit vulnerabilities in systems occur among disgruntled employees and ex-employees and the persistence of this threat is testimony to the need for on-going vigilance. Neumann (1994) reports, for example, that insider manipulation of currency transactions via computer cost Volkswagen \$260 million while a fraudulent EFT transfer, which would have cost the Bank of Switzerland \$54 million, was only averted at the last minute. While garden variety electronic thefts, destructiveness, and espionage in legacy systems are serious in their own right, more recently abusers have targeted the Internet. In the last few years, Internet connectivity and security on the World Wide Web pose the most significant threat for many organizations (Arnum, 1995). The possible strategic benefits from electronic commerce are clearly attractive to many firms, but some are entering into this venture without fully recognizing the potential aftereffects of lax security.

The potential for security exposure from viruses crossing over networks, which know no international boundaries, for instance, is virtually unlimited. Although outsiders (many of whom, of course, are hackers) have historically been a relatively small percentage of computer abusers (Hoffer and Straub, 1989; Gips, 1995; King, 1995), the persistence of their attacks and their resistance to deterrent countermeasures makes them particularly dangerous (Straub, Carlson, and Jones, 1992; Straub and Widom, 1984). They can attack systems directly or set loose viruses, which estimates suggest that viruses are successfully attacking systems over 20,000 times per year in France (Forcht, 1992) while in the US over 70% of organizations are experiencing serious virus attacks (Panettieri, 1995). Moreover, the vast majority of managers say that systems risks have escalated in the past five years and that their organizations have suffered financial losses from computer abuse (Panettieri, 1995).

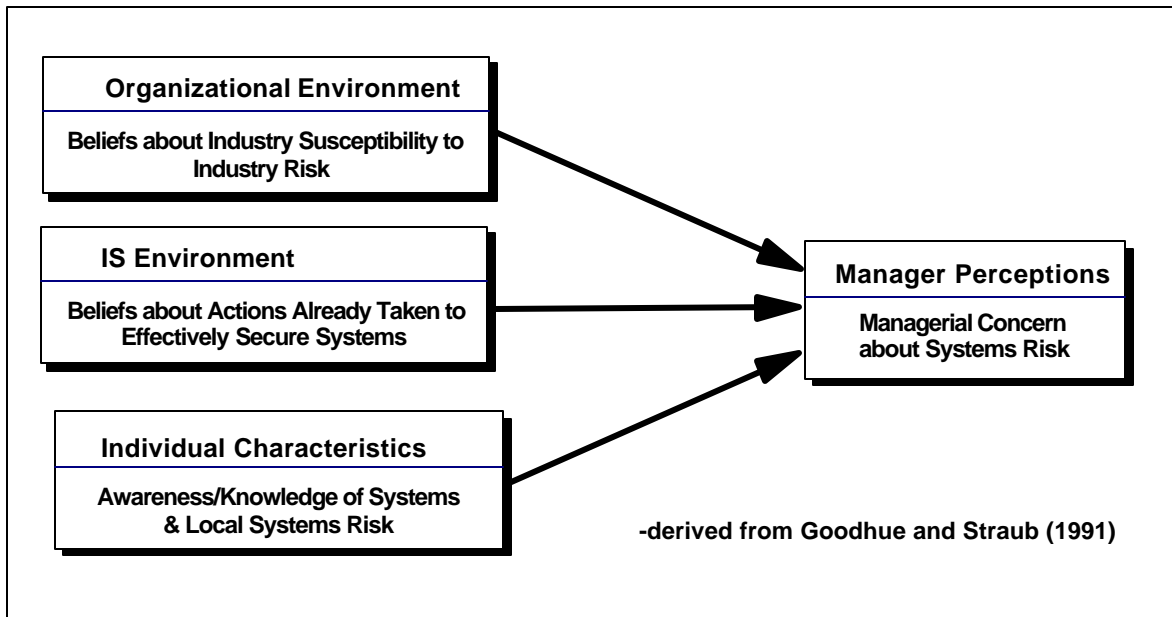
In spite of the seriousness of systems security risk from disasters and computer abuse, many organizations are either completely unprotected or insufficiently protected. Numerous surveys and other studies report this same lack of preparedness over and over again (e.g., Loch et al., 1992; Hoffer and Straub, 1989; Brown, 1993).

## **Prior Thinking about Systems Risk**

If the threat is so clear, then how can it be true that both IS and general managers may be under-prepared in coping with systems risk? If managerial perception of systems risk is lower than it should be, why is this the case? How does a manager develop a sense that his or her risk-cost tradeoff is well balanced? While a few studies have addressed this issue conceptually, one study has explored the issue from both a theoretical and empirical perspective (Goodhue and Straub, 1991). They argue that managerial concern about the organization's security is a function of: (1) risk inherent in the industry, (2) the extent of the effort already taken to control these risks, and (3) individual factors such as awareness of previous systems violations, background in systems work, etc., as shown in Figure 1. Independent corroboration of these factors has been reported by Dixon, Marston, and Collier (1992).

How can managers' consciousness about security risk be heightened? If this model is accurate, then clearly it is necessary to alter managers' perceptions of the three underlying components of risk in order to affect their overall perception of risk. Having a firm grasp on the level of systems risk to which the industry as whole is exposed, reflected in the "Organizational Environment" construct in the model above, would clearly be helpful. How managers develop beliefs about industry risk, however, is beyond the scope of the current research because it involves relatively straightforward reading and/or sharing of knowledge of the risk among industry groups.

But the second and third model components, "IS Environment" and "Individual Characteristics," offer managers a good opportunity for learning and, hence, improvement. Managers should very likely be well informed as to the local incidence of computer abuse and susceptibility to damage, as shown in the "Individual Characteristics" component of the model. That one's system was attacked three times last month, once successfully penetrated, causing a loss of one hour of system availability is the type of localized knowledge we are referring to. As we shall see later in the section entitled "Intervention Elements," such knowledge is instrumental in *managerial risk analysis*.



*Figure 1. Model for Managerial Perceptions of Security Risk*

The second model component, “IS Environment,” reflects managers’ basic understanding of the range of technical and managerial controls that can cope with risk from disasters and computer abuse. It also reflects actions that can be taken based on that knowledge. If the firm’s customer base has on-line connections to the firm, for instance, there are hard box solutions such as secure modems that can be used to address security issues; software solutions, such as passwords, may also be acceptable. This knowledge determines the *alternatives* to be considered in security response decision-making.

In addition, these areas are of greatest need in that manager’s knowledge of actions to reduce local systems risk has been found to be fragmentary and incomplete in numerous prior studies (Loch et al, 1992 ; Straub, 1986a; Straub, 1986b). *If such knowledge of local threats and risk-lowering actions can lead to effective planning and implementation, then prospects for successfully dealing with systems risk should be greatly enhanced.* In order to understand how business practitioners can manage systems risk, it is first necessary to appreciate the full range of possible action.

### **Effective Actions for Managing Systems Risk**

For years, the received wisdom of security experts is that countermeasures, strategies that adopted to reduce systems risk, fall into four distinct, sequential activities, namely: (1) deterrence, (2)

prevention, (3) detection, and (4) recovery (Parker, 1981; Martin, 1973; Forcht, 1994). Not surprisingly, perhaps, these four classes of sequential actions have a strong theoretical basis.

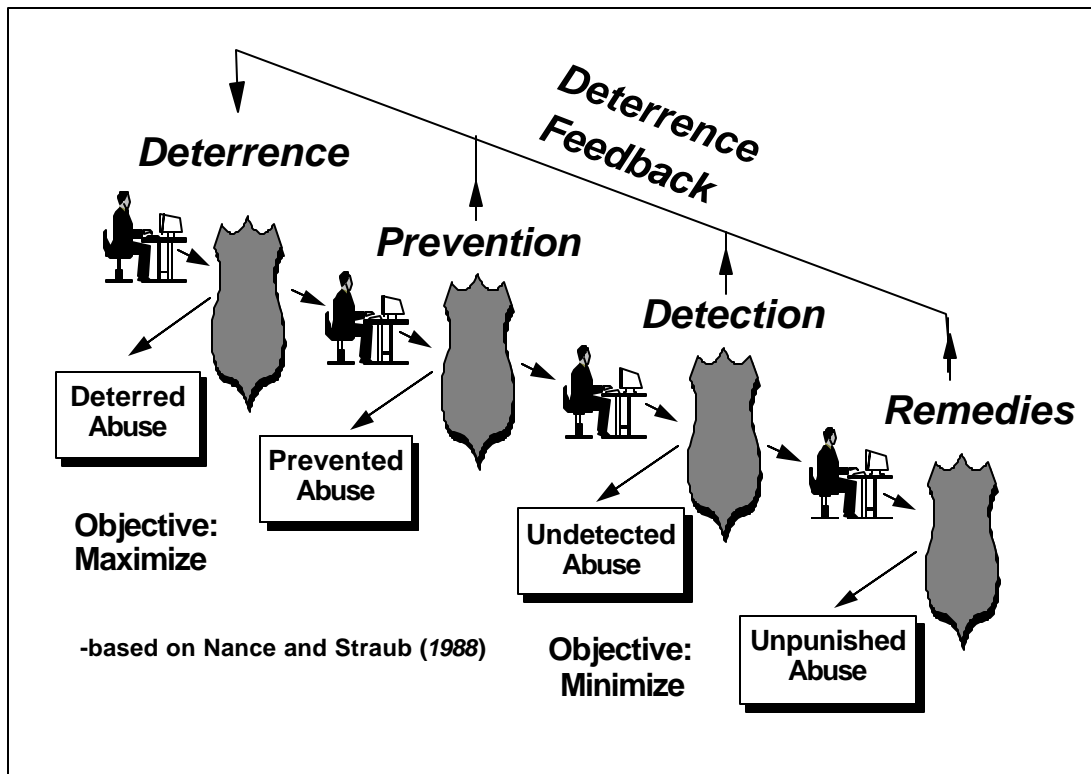
The theory that best explains the effectiveness of these countermeasures is general deterrence theory. Used in the study of criminals and other anti-social personalities, the theory is well established in criminology (Blumstein, 1978; Pearson and Weiner, 1985). It posits that individuals with an instrumental intent to commit anti-social acts can be dissuaded by the administration of strong disincentives and sanctions relevant to these acts. In more easily understood terms, active and visible policing is thought to lower computer abuse by convincing potential abusers that there is too high certainty of getting caught and punished severely.

General deterrence theory has been applied successfully to the IS environment by Straub and his research partners (Straub, Carlson, and Jones, 1994; Straub, 1990; Straub and Nance, 1990; Hoffer and Straub, 1989). The basic argument in this work is that information security actions can deter potential computer abusers from committing acts that implicitly or explicitly violate organizational policy. Moreover, they have found empirical evidence that security actions can lower systems risk. Specific application of general deterrence theory to information security is based on the underlying relationship between activities of managers and that of computer abusers (Nance and Straub, 1988). Figure 2 illustrates the range of possible security actions and their interrelationships.

With respect to risk from computer abuse, this model asserts that managers are themselves the key to successfully deterring, preventing, and detecting abuse as well as pursuing remedies and/or punishing offenders for abuse. It should be noted that these constructs and inter-relationships, which are explicitly expressed in Figure 2, "The Security Action Cycle," are implicit in general deterrence theory, specifically in the lag effects of policing actions on subsequent anti-social acts.

A certain portion of potential system abuse is allayed by **deterrent** techniques, such as policies and guidelines for proper system use and by reminders to users to change their passwords. Deterrent countermeasures tend to be passive in that they have no inherent provision for enforcement. They depend wholly on the willingness of system users to comply. Security awareness programs are a form of deterrent countermeasure which deserve special mention here because educating users as well as their superiors about security yields major benefits. These sessions convey knowledge about risks in the organizational environment; emphasize actions taken by the firm, including policies and sanctions for

violations; and reveal threats to local systems and their vulnerability to attack. A major reason for initiating this training, however, is to convince potential abusers that the company is serious about securing its systems and will not treat intentional breaches of this security lightly. In essence, potent security awareness training stresses the two central tenets of general deterrence theory — certainty of sanctioning and severity of sanctioning (Blumstein, 1978).



*Figure 2. The Security Action Cycle*

When potential abusers choose to ignore deterrents, the next line of system defense is **preventives**, like locks on computer room doors and password access controls. Preventives are active countermeasures with inherent capabilities to enforce policy and ward off illegitimate use (Gopal and Sanders, 1992; 1997).

If an abuser successfully penetrates the first two lines of system defense, the organization needs the capacity to **detect** misuse. Proactive security responses such as suspicious activity reports and system audits are examples. Virus scanning reports would be other examples. Reactive responses include detective work after a documented breach in security. The primary objective of this security response is to gather evidence of misuse and to identify perpetrators.

Finally, an effective security program should be able to **remedy** the harmful effects of an abusive act and to punish the offender(s). Internal actions in this stage include appropriate responses to offenders in the form of warnings, reprimands, and termination of employment. Legal actions include criminal and civil suits. As will be seen in a moment, all of these organizational responses lead to a downstream effect of deterring future computer abuse. Other remedies, like software recovery facilities that assist in this process, are technical remedies for recovery which do not result in deterring future abuse, *per se*. From the perspective of general deterrence theory, these four kinds of defense can contribute dynamically to a subsequent deterrent effect. That is, potential abusers become convinced of the certainty and severity of punishment for committing certain acts when the effectiveness of the system security is obvious or when it is communicated to them. The **deterrence feedback** loop, in short, strengthens deterrence by ensuring that potential abusers become aware of consequences of abuse.

Managers, both systems and general managers alike, are directly involved in identifying those who violate security (Straub and Nance, 1990; Hoffer and Straub, 1989) and in applying the appropriate actions to deter, prevent, detect, and remedy computer abuse. Certain of these activities are particularly onerous in terms of time and effort expended. Detective activities, for example, require the investigation of suspicious activities, most of which prove to be false positives in suspicious incidents reports. Knowledge of the most effective combination of disincentives and other strategies for managing risk, is, therefore, of special value.

There is limited evidence in practice for the effectiveness of these techniques despite the strong theoretical basis (see Straub, 1990, however). This raises a critical research question: Are managers fully aware of the range of generic security actions that research links to lower systems risk (Straub, 1986b; 1990)? Lack of awareness would be suggestive about the probity of the Goodhue-Straub model of security concern (1991). Correcting this could also lead to managerial action plans. Beyond lack of awareness, it seems likely that managers will stress certain countermeasures over others. Prior work suggests that preventives would be best known and other countermeasures less understood.

Ancillary research questions arise from this contrast: Can security awareness programs that stress theoretically-grounded countermeasures affect manager's thinking about security and will managers actually adopt into practice forms of planning that reflect such theoretically-grounded countermeasures? Can other theory-based security planning techniques affect how managers plan for

security? Answers to these questions would be insightful in that managers may or may not be swayed by and induced to put into practice theory-based approaches to lowering risk. Accordingly, we studied the following two propositions:

**Proposition 1: Managers are aware of only a fraction of the full spectrum of actions that can be taken to reduce systems risk.**

**Proposition 2: Managers exposed to theory-grounded security planning techniques will be inclined to employ these in their planning processes.**

## **Research Approach**

To empirically study these propositions, comparative qualitative studies were conducted in two Fortune 500 firms with information technology services in the southeastern United States. Because security is an extremely sensitive subject for many organizations, firm identity has been disguised. From the standpoint of research design, Customer Processing Company (CPC) was similar to Customer Data, Inc. (CDI) in enough respects to make comparisons meaningful. Both are Fortune 500 information services companies. Their businesses involve processing data and marketing this value-added product to customers. Both organizations have been in the business for many years, have approximately the same total revenues, and structure information delivery in a markedly similar fashion. Information security had been staffed at both organizations within the IS department for many years. In both, disaster recovery plans were operational, whereas application security was less well developed. What is, perhaps, even more important is that neither organization had long term experience in offering user/manager education in security awareness at the time of the qualitative studies. Because each of these organizations presented, in effect, a green field setting for this important aspect of security, it was possible to compare their beginning points and progress toward strengthening security along several lines. A comparison of the firms, propositions investigated, and methods employed appears in Table 1.

<b>Firm Pseudonym</b>	<b>Abbreviation</b>	<b>Proposition Explored</b>	<b>Methods Employed</b>	<b>Period</b>
Customer Data, Inc.	CDI	1	Interviews	4 months
Customer Processing Co.	CPC	1 & 2	Action Research	15 months

**Table 1. Comparison of Qualitative Studies at Two Sites**

## **CDI Study Details**

In Customer Data, Inc. (CDI), 30 intensive interviews were conducted with all levels of management, including three Vice Presidents over a four month period. The interviews were conducted in a southeastern city, two midwestern cities, and a western city. Professionals working with systems on a daily basis, both in the IS department and in functional areas, were also a critical component of the sampling. Interviews lasted from one hour to over two hours. The interview script that was employed appears in the Appendix. There were several specific questions that attempted to gain insight into the security planning process used at the firm. Question 4 in the interview script illustrates the straight-forward approach taken in these questions: “If you were asked to plan for some new security measures at the company, how would you go about doing this? Are there certain stages or phases that might be involved in your planning for improved security?” (The underlining in the script was intended to remind the interviewer to stress these words).

To bring a measure of objectivity to this data, interviews were transcribed and thematically coded for indications that participants were cognizant of the meaning or value of one of the particular countermeasures. They were then qualitatively analyzed for dominant and sub-thematic patterns. The content analysis process was relatively simple in that one coder was used. The coder was intimately familiar with the countermeasure themes as a result of fifteen years of research and consulting experience in the computer security field. Whereas multiple coders would have been preferable from a methodological standpoint, the sheer volume of data accumulated in both studies meant that this approach was too costly.

## **CPC Study Details**

CPC differed in one regard from CDI which made it exceptionally valuable for this comparative qualitative study. Through an intervention, it became possible to educate top managers and other professionals at CPC in concepts and principles of theory-grounded models of security planning and then to systematically observe if and how they used this information in their later security planning. Action research, an interpretive mode of inquiry, was used to analyze the data in this case.

Thirty-seven top managers, middle managers, and other professionals were involved in the comparative study, which took place over a 15 month period. One major source of information was a mid-level security planning team which held regular project meetings for 15 months. This project team was composed of 10-12 managers/professionals representing business units such as marketing and operations as well as systems development professionals such as telecommunications and systems R & D analysts. The team was charged with investigating a wide range of security options to protect the firm's sensitive data. Team members would also implement those security options selected for investment by top management.

In addition, meetings with top management, including the President and several levels of Vice Presidents, were held on a monthly basis during the study period. These sessions were both informational and decision-making sessions. Investigation and approval of security initiatives, hence, had continuous top management involvement.

Meeting minutes, notes, internal memoranda, presentation overheads, analyses of security initiatives, and CPC customer interviews provided a rich source of data for documenting the planning effort and multiple chains of evidence with respect to the propositions. Even though there were no formal interviews with the project team or top management, all told, approximately 1000 pages of documentation were amassed over the 15 months of the project. Subjective, interpretive analysis of this data revealed extremely interesting patterns in how the participants learned about and subsequently responded to the organizational responses embodied in the Security Action Cycle.

The rich data source that resulted from CPC security initiative was interpreted in a similar fashion to that of CDI data. Major themes related to the Security Action Cycle were pattern analyzed and conclusions were drawn from this analysis.

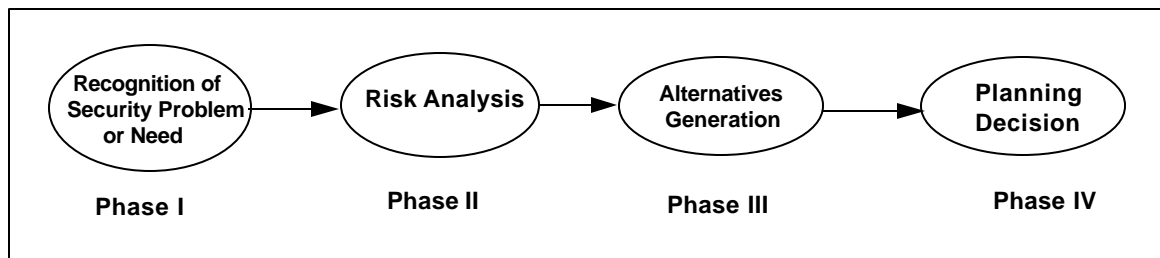
### **Intervention Elements**

Proposition 2 posits that when managers have theory-based planning models for strengthening security, managers will be motivated to utilize these tools. In creating the intervention during the action research, these models were based on the best conceptual and theoretical evidence we have on the nature of systems risk and how to cope with it.

There were three elements to the intervention implemented at CPC: (1) a security risk planning model, (2) a security awareness training program, and (3) a Countermeasure Matrix model. Each of these will be explained in greater detail below.

### **Intervention Element #1: The Security Risk Planning Model**

To deal with managers' need for a deeper understanding of the full spectrum of risk management responses, the Security Risk Planning model, grounded in Baskerville (1993) and Simon (1960) and presented in Figure 3 below, served to guide the overall security planning effort. This model derives its structure from Simon's model of decision-making (1960). Building from a definition of information security planning, the model places risk analysis in its proper logical position as a bridge between problem formulation and generation of alternatives and preceding the planning decision phase. This normative model of the entire planning process includes not only risk analysis but also the constituents of other critical stages and their outcomes. This model is presented in Figure 3 and constituents of each of the phases, as well as an additional phase for implementation, are shown in Table 2 below.



*Figure 3. Phases in Security Risk Planning*

Current thinking and practice were also lacking in an effective mechanism to evaluate the fit between business needs and potential solutions. At present, the literature advocates only a crude cost-benefit mechanism that falls far short of the kind of intellectual tools that would lead to high quality, scientific assessment and good planning decisions (Baskerville, 1991). The problem with such present first generation tools (Baskerville, 1993) is that they are atheoretical (Hoffman, 1989). As simple heuristics that estimate rough-cut costs of a unsecured system and benefits from implementing security

controls, they play down or completely ignore the behavioral side of the phenomenon of computer abuse. Present atheoretical techniques are also incapable of evaluating the synergy offered by combinations or sets of security controls. In fact, practitioner and academic interest in information security (IS) planning has been marginal. Planning for security is mentioned only briefly in this literature (viz., McLean and Soden, 1978; Steiner, 1979, 1982; King, 1984; Venkatraman, 1985-86; Ramanujam and Venkatraman, 1987; Lederer and Sethi, 1991). These studies neither detail the nature of security planning nor the process stages required for a successful planning effort.

Likewise in the more specialized security and control literature, the issue of security planning has not been dealt with. Although Parker (1981; 1983), Fisher (1984) Caroll (1987), Baskerville (1988; 1993), and Forcht (1994) all discuss means by which threats to systems can be identified and countermeasures proposed, they do not discuss this process as a planning process *per se*. Stages in a normative planning process are not articulated in this literature nor are the desired outcomes of the stages.

<i>Phase</i>	<i>Phase Name</i>	<i>Description</i>
<b><i>I</i></b>	<b>Recognition of Security Problems</b>	The identification and formulation of problems with respect to the risk of IS security breaches or computer disasters
<b><i>II</i></b>	<b>Risk Analysis</b>	The analysis of the security risk inherent in these identified problem areas; threat identification and prioritization of risks
<b><i>III</i></b>	<b>Alternatives Generation</b>	The generation of solutions to meet organizational needs specified during risk analysis
<b><i>IV</i></b>	<b>Decisions</b>	Matching threats with appropriate solutions; selection and prioritization of security projects
<b><i>V</i></b>	<b>Implementation</b>	Realizing the plans by incorporating the solutions into the on-going security of the organization

***Table 1. Description of Phases in the Security Risk Planning Model***

Baskerville (1993) argues that planning for security should ideally be incorporated systems development and security controls designed at the logical systems level in parallel with actual system functionality. Recognizing that systems projects seldom unfold in this fashion, Baskerville goes on to

argue that *ex post* security enhancement can indeed be undertaken for existing and legacy systems. The broad outlines of his planning process are not dissimilar to those shown in Figure 3.

Other than Baskerville (1993), the scholarly and consulting literatures on security do not provide a commonly agreed upon conceptual model for the security planning process. Much of the literature, indeed, specifies in detail only one of the central activities of the process, namely, risk analysis (Parker, 1981, 1983; Fisher, 1984; Carroll, 1987; Badenhorst and Eloff, 1989; Eloff, Labuschagne, and Badenhorst, 1993). Whereas von Solms, van de Haar, von Solms, and Caelli (1994), de Konig (1995), and others discuss various types of planning (e.g., disaster recovery planning vis-à-vis contingency planning vis-à-vis physical security planning, etc.), there is little in the public domain describing an overall approach to security planning and evaluation or the specific details of this process.

The Security Risk Planning Model was, *de facto*, the organizing principle behind the security initiative at CPC. Needs were determined in the early phases of the project and decision choices were made after a significant effort in alternatives generation. This approach was articulated in the early stages of the project and followed rather closely as the project progressed. The implementation phase of the project followed the straight-forward planning phases, as in most projects.

## **Intervention Element #2: Security Awareness Program**

Phase I of the security risk planning model just discussed requires that decision-maker awareness of industry standards for security is sufficient, as is knowledge of local security conditions and available countermeasures within one's own firm. During this phase, managers and security professionals should identify and formulate problems with IS security breaches or computer disasters in the organization, as suggested by the Goodhue-Straub Model for Managerial Perceptions of Security Risk (1991; Figure 1 above).

An effective way of achieving this is through security awareness training, or the training of managers and other professionals in proper use of system assets. In this training, security specialists review with employees policies (if they exist), system authorizations, conditionalities for use, methods for changing passwords, penalties for security breaches, and other topics that have a bearing on preventing misuse of system assets. The training should also make participants aware of the general effectiveness

of deterrent, preventive, detective, and remedial countermeasures in lowering systems risk, as articulated in the Security Action Cycle (Figure 2 above).

Forward-looking and proactive security awareness program are exceptional in most industries. Fewer than half of organizations likely have active security awareness programs in place; moreover, about two thirds believe that information security is not a significant issue (Kearns, 1994). Such views fly in the face of commissioned studies that have consistently concluded otherwise (Kusserow, 1984; American Bar Association, 1983; Dixon, et al., 1992).

At CPC, security awareness training was not conducted as a specifically designated training session; nevertheless, the knowledge that would be imparted in formal sessions was communicated informally to team members and management by both the resident security staff and the action researcher during meetings and work sessions in the early phases of the project.

### **Intervention Element #3: Countermeasure Matrix**

In making decisions in Phase IV from among the security alternatives generated in Phase III, managers may enhance their decision-making with the assistance of a “Countermeasure Matrix,” an example of which is shown below in Table 2. Many of the intellectual tools to improve this phase focus on risk analysis of security threats (Eloff, Labuschagne, and Badenhorst, 1993; Wood, 1988). Two French tools, MARION (Méthode d'Analyse de Risques Informatiques et d'Optimisation par Niveau) and MELISA (Méthode d'Evaluation de la Vulnérabilité Résiduelle des Systèmes), for instance, are useful in determining where the vulnerabilities in a system lie and in assessing their relative effects. While, the UK assessment methodology CRAMM goes beyond risk analysis to recommend prioritized countermeasures for assessed risks (Farquhar, 1991), implementation requires in-depth security knowledge (Farquhar, 1991). Like the “Countermeasure Matrix,” BDSS is another theory-based tool that suggests appropriate safeguards (Baskerville, 1993).

Whereas the problem recognition and alternatives generation phases have received some attention in the general management literature, the planning decision phase (Phase IV) has received less treatment in the security literature (see Parker, 1981, 1983; Fisher, 1984; Carroll, 1987; Wood, 1988; Baskerville, 1988, 1993; Forcht, 1994, for example). Thus, new intellectual tools that can assist managers in matching security risk with an appropriate set of security controls is useful. Moreover, as is

evident from the preceding discussions, such a tool should be based not on heuristics alone, but, if at all possible, firmly grounded in theory.

The "Countermeasure Matrix" model, hence, is a theory-based, analytical tool for evaluating the overall effectiveness of security options. Table 2 is an illustration of how this model would be applied to a particular security problem or need.

To understand the essential features of the technique and see how these features might be used in practice, consider the following situation. Let us assume that an organization has decided to give customers electronic access to their mainframe product/pricing database and has had customers sign non-disclosure agreements as part of a contractual relationship. Let us further assume that the company would like to limit the extent to which non-customers and competitors can gain access to this same data. Thus, the firm wishes to discourage non-customers and competitors from accessing the database while making the database accessible to customers. Should security fail for some reason, the firm would also like to be able to identify the offender and seek restitution in the courts.

A requirement for effectively using the matrix is that some persons or groups of persons in the organization have sufficient expertise to be able to identify the full range of security solutions that could meet the firm's needs in this case. Let us make the assumption that viable alternatives have been assembled by this expert and that two security approaches — PINs or personal identification numbers and token-exchanging modems are selected for further evaluation.

These proposed security solutions demonstrate how the matrix might be populated. The matrix is formed by assigning methods in the Security Action Cycle to the row headings and proposed organizational solutions to the column headings. The cells in the matrix allow managers to compare the effect of proposed solutions across the security countermeasures of deterrence, prevention, detection, and remedies. PINs have been evaluated as effectively meeting the goal of deterrence because individuals identify themselves to the computer system via this token. Thus, it may be assumed that individuals recognize that every interaction with the system can be linked directly back to them. The token-exchanging modems, conversely, are a "hard box" device that in an open office may be shared, lost, or stolen and, hence, not necessarily identify access by specific individuals. Therefore, it has little or no deterrent effect. Token-exchanging modems and PINs are both capable of controlling access to the system, data, or files and are noted, thus, as effective preventives. PINs allow security officials to

trace individuals, associate particular persons with particular abuses, and institute corrective and/or legal action. For this reason, PINs are classified as meeting detective and remedial goals. Since token-exchanging modems may not be unambiguously associated with individuals, their detective effect is limited to identifying compromised modems. Their remedial effect, thus, is present, but highly limited.

Countermeasures	<b>Security Option A-- Authentication via Personal Identification No.</b>	<b>Security Option B-- Authentication via Security Modem Device</b>
<b>Deterrence</b>	Request for PIN from user; recognition by user that an individual can be personally identified	
<b>Prevention</b>	Access for valid PIN only	Access for valid token-exchanging modems only
<b>Detection</b>	Identification of perpetrator; log of illicit activity	Identification of compromised modem; log of illicit activity
<b>Remedies</b>	Recovery from losses; prosecution of identified perpetrator	

*Table 2. Application of the Countermeasure Matrix to a Problem*

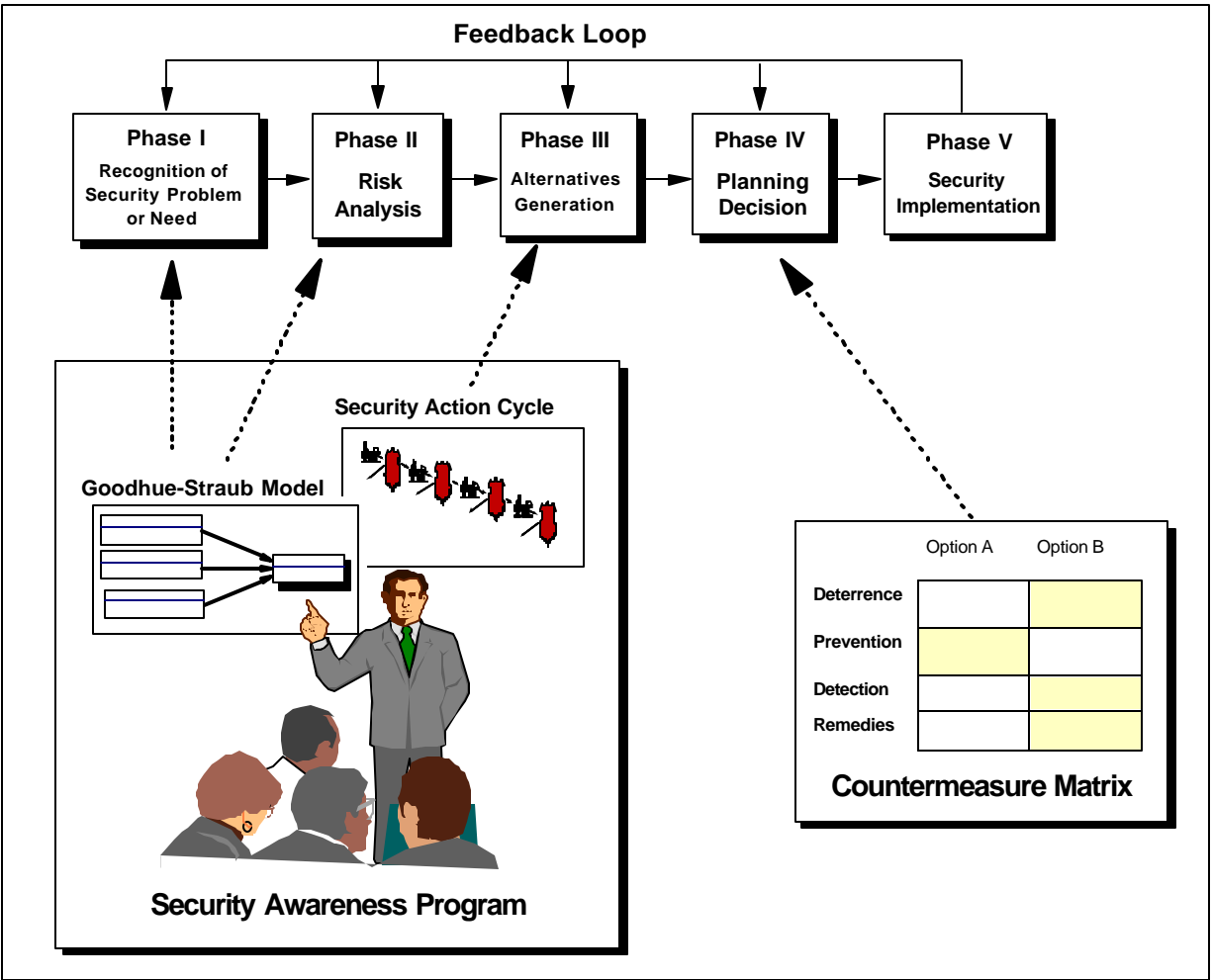
The use of the "Countermeasure Matrix" highlights strengths and weaknesses of proposed security solutions to meet the firm's needs. All things being equal, the PIN solution in Table 2 meets more of the security goals of the organization than the token-exchanging modems. When planning for security, therefore, managers can use the matrix as a technique for assessing both the short and long term effect of security options by considering the immediate effect of deterrence, prevention, etc. as well as the downstream feedback effects. When a decision must be made between options, the application of the matrix provides guidelines for a rational choice.

The matrix can also suggest how the organization can respond if certain contingencies must be taken into account. If there would be reason to suspect that PINs might not always be tightly guarded by customers and might fall into the hands of competitors, for example, the matrix indicates that token-exchanging modems **in addition to** PINs would be a good means by which to prevent unauthorized access. To completely compromise the system in this situation, competitors would also have to acquire token-exchanging modems.

## **Placing the Interventions into their Overall Security Context**

As Figure 4 shows, the three interventions being proposed and studied here fit into the context of security planning in a relatively simple way. The Security Risk Planning Model provides the baseline of phases I-IV to which are added the implementation phase (V) and feedback loops in Figure 4. Awareness programs aid managers and professionals in identifying security issues (Phase I). Awareness is the first charge of security training and one of the tools that can structure this discussion and help to identify problems is the Goodhue-Straub model (Figure 1). The model presents to employees the general concept that risk and security awareness are a function of both their industry and firm's susceptibility to abuse and the countermeasures taken to control risk. Risk analysis (Phase II) is affected by security awareness programs in that these programs inform managers and professionals about specific local susceptibility to certain threats, as shown in the "Individual Characteristics" component of the Goodhue-Straub model (Figure 1). They also serve to inform users about the entire process of designing effective organizational responses (Phase III). This phase conveys knowledge of the possible actions that can be taken to reduce risk, i.e., the "IS Environment" or second component of the Goodhue-Straub model (Figure 1). The Security Action Cycle is an example of the actions that can be taken. Knowing and using this model can help in generating security alternatives. Finally, the Countermeasure Matrix is proposed as a useful analytical technique for making the final decision as to which option provides maximal security impact (Phase IV).

Once security is implemented, feedback from the relative success of the project can reinforce knowledge gained during the earlier phases or it can assist in balancing expectations in subsequent projects (Senge, 1990).



**Figure 4. Interventions in their Overall Security Context**

### Method of Comparison and Manipulation

The basic method used in the research was that of comparison and manipulation (Cook and Campbell, 1979; Yin, 1994). Because proposition 1 was examined at both firms, the comparison allows us to determine how managers frame questions dealing with improved security and, at the same time, to ensure that the firms did not demonstrate wide variation in this fundamental aspect of security planning. If the firms do not differ in these underlying initial conditions, then the argument that propositions found to be true in both settings could apply to settings beyond the sample is more persuasive.

Manipulation occurs in laboratory or field experimentation when reputed causes are consciously manipulated and effects observed in as unobtrusive manner as possible (Stone, 1978; Fromkin and

Streufert, 1976). In action research, there is also conscious manipulation of reputed causes; in this situation, though, the researcher is an active and obvious observer of the phenomenon under scrutiny (Jenkins, 1985; Yin, 1994). Evidence in favor of propositions is strengthened when a researcher manipulates a reputed cause and subsequently observes the predicted effect, as in the case of the interventions in the present study.

### **Validity of Research Approach**

It should be noted that while the current research did not strictly follow the classic stages of research as described by authors such as Jenkins (1985), it is clearly within the purview of action research studies now being conducted (Baskerville, et al, in press). Both projects were originally consulting projects, which, at the same time, were consciously conceived as research projects. The participating organizations were aware that the data gathered would, ideally, find its way into academic papers dealing with security. Moreover, the signed non-disclosure documents did not preclude the possibility of wider dissemination of this information so long as company names were disguised. In fact, both firms were very helpful in reading, reacting to, and eventually approving versions of the paper for submission to academic journal review.

The research varied from classic research stages in one other respect. While the research questions were clear from the beginning of the first project, the design itself evolved. The combination of action research and interviews to study managerial responses to security situations progressed in an organic way rather than being part of any preset, original design. Nevertheless, the value of triangulating on the phenomenon through two markedly different methods is well known (Fielding and Fielding, 1986) and we were able to capitalize on these research capabilities in this case.

With respect to the validity of the action research component, it is critical that models being examined are integrated into the process (Schein, 1987). Participants in the CPC project learned about the models in at least three ways. First, they learned *about* the model during formal presentations during meetings. Second, they learned *from* the models by seeing their immediate problems being analyzed through the models. Finally, they learned *how to use* the models so that they could analyze similar situations later. All three of these forms of learning occurred during the action research.

Another primary characteristic of successful action research is that the immediate problem has been solved (Schein, 1987). As we shall shortly see, this proved to be the case for CPC. Decision-makers were able to consider a wide range of security solutions and to focus on those that met their needs.

## Qualitative Data Analysis

### Proposition 1: Interviews at Customer Data, Inc. (CDI)

Based on interpretation of the data gathered through the numerous interviews of managers at CDI, there are grounds for arguing that practitioners feel comfortable with some of the countermeasures embodied in the Security Action Cycle, but not all. Namely, **recovering** from and **preventing** a security “incident” were identified by more than 75% of the participants as managerial actions that can be used to deal with systems threats. One participant in this 75% group felt that **remedial** actions needed to be taken after a break-in. He expressed this sentiment in the following way:

*If there is evidence of break-in, maybe looking outside this organization as to who and how but if there is no evidence immediately of break-in, then we try to find out who had access to that information....*

Another member of this group commented on how **preventives** were invoked:

*[To attach to the network, there is a ...] user authentication procedure you have to go through just to get on the network. Those are built into the product....*

Three countermeasures of effective risk management were missing from nearly all of the respondents’ concepts of good information security, however. Proactive **detective** activities were seldom cited. The **feedback** effect of sanctioning activities was likewise not readily understood by this group of practitioners, this learning effect never being mentioned by study participants in any of the interviews. Finally, even though the first phase of risk management, **deterrence**, was mentioned, it appeared only in an indirect way. Typically, it was alluded to in statements that greater user awareness would be desirable so that preventive measures would work better and so that detection would be surer

if a break-in occurred. One manager, for example, indicated that it was important to be able to have close communications with human resources to prevent fired employees from continuing to access the network:

*I would make sure that the local area networking administration has a direct pipe in with human resources because we need to know who is going and who is coming and who went and why and when they took them off the network.*

In general, interviewees were not aware of the impact of **remedial** countermeasures on potential abusers. They were much more aware of the recovery aspects of remedies. From the standpoint of influencing future behavior of potential abusers, however, being capable of recovering from a breach is not really relevant.

One exceptional manager's view illustrates how an insight into the Security Action Cycle could affect overall security planning. Unlike other interviewees, this manager noted that it was critical to internally discipline insiders who intentionally abused the system. He argued that a forceful organizational response was important...

*...because people want to find out who is responsible - the people who may be looked at first if it's an incident that is not attributed to a particular user, my guys have access to everything. Not only my people here, people who I work with in the networking business from other units. You know the supervisors in the wide area and the LAN so I think we would come under scrutiny. Especially if there seem to be - like when someone breaks into a house, if someone is harm or assaulted in the home, first they see if there was any type evidence of break-in. If there was no evidence of break-in, maybe it was an inside thing. Someone knew the family or had a key or something like that.*

He goes on to observe that this "hanging tree" effect would "**deter**" future abuse. Remarks like these indicate clearly that he had a keener intuitive sense for the **feedback** created by countermeasures than others did.

What is instructive about the perceptions of this firm's managers is that an overwhelmingly positive attitude toward security was not accompanied by a thorough understanding of available security responses. In spite of a strong consensus that the firm lacked an acceptable level of security awareness, interviewees were not generally clear as to how a security awareness program, for example, would have downstream, learning impacts on the major systems threats.

**Proposition 1:**  
**Action Research at Customer Processing Company (CPC)**

To study managerial knowledge of security and whether theory-based concepts and principles of the Security Action Cycle would actually be adopted by managers, a second qualitative study was conducted at Customer Processing Company (CPC).

In the early planning stages, CPC participants revealed the same disposition as those at CDI. Methods for **preventing** access to sensitive systems were far and away the most frequently discussed. Top managers stressed the need to find controls that would inhibit unauthorized access and to implement them as soon as possible. One security team member expresses this view when he reports on the security possibilities of Automatic Number Identification (ANI):

*ANI/Caller ID are telecommunications technologies that allow the telephone number of the caller to be electronically transmitted to the party being called. They also provide the ability to display the number at the receiving end. [These technologies would allow CPC...] to receive, and verify, the telephone...requesting access to [our] database.*

Over the three month period in the early stages of security planning, methods for preventing access were mentioned an order of magnitude greater than the next class of responses.

**Remedies** in the event of a security breach were discussed next in frequency. Team members focused on how the firm should proceed in recovering from damage from a major security incident. Of particular concern were adverse media coverage of any security breaches, ways to limit the damage, and correct any underlying problems. Again, as in the case of CDI, the remedies that were identified were closely associated with recovery mechanisms, which have little to no impact on downstream deterrent effects.

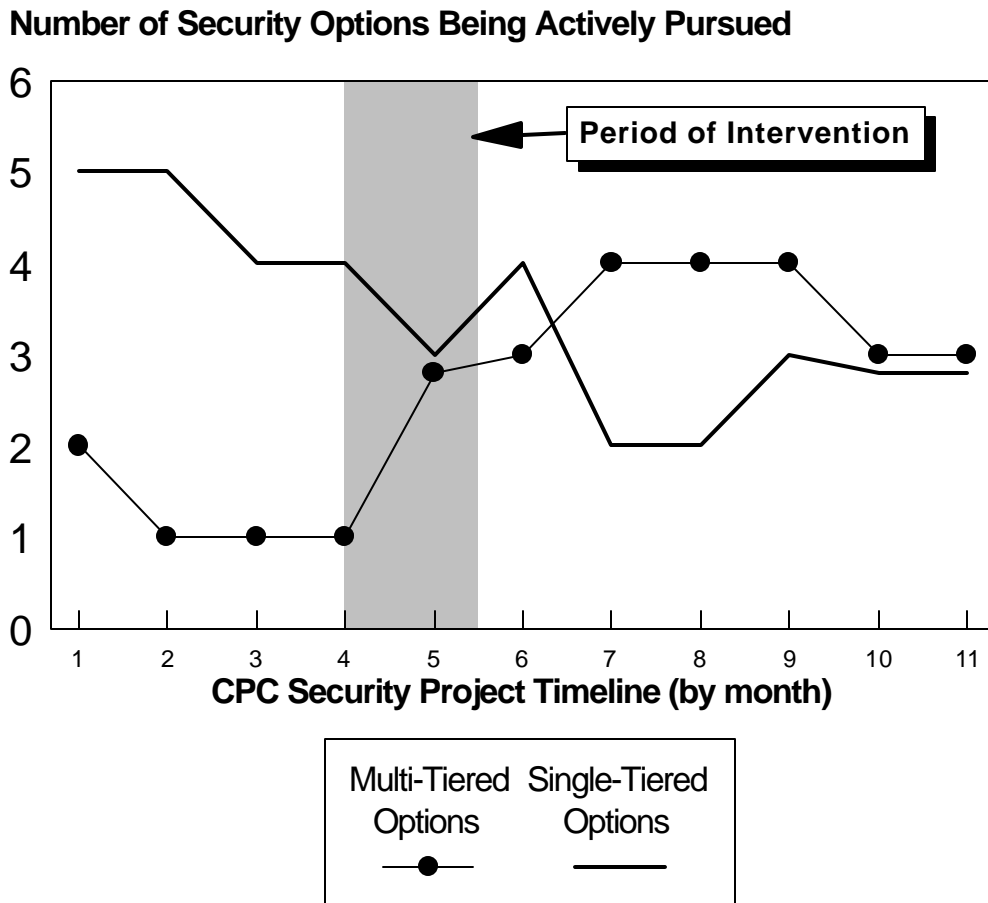
Early in the security planning at CPC, little attention was paid to proactive **detection** of compromised security. Avoiding abuse through passive approaches (**deterrents**) was likewise infrequently hailed as a security requirement.

**Proposition 2:**  
**Action Research at Customer Processing Company (CPC)**

The intervention at CPC included a series of mini-educational sessions and reports designed to introduce the spectrum of responses in the Security Action Cycle to both the top management and project teams. Thus, during the 5 ½ month period through the first half of the project, it was possible to introduce all three elements: intervention element #1, the Security Risk Planning Model, intervention element #2, security awareness training, and element #3, the Countermeasure Matrix.

With respect to element #3, the multi-tiered nature of the Security Action Cycle was stressed during meetings and reporting sessions. An attempt was made to convey the basic theme that countermeasures such as token-exchanging modems are restricted to a **single-tiered** effect since they are designed only to *prevent* unauthorized access. The Countermeasure Matrix was the specific modeling mechanism for making this concept concrete. A control such as a Personal Identification Number (PIN) has an impact on **multiple tiers** in that it prevents unauthorized access, provides a means to detect and punish an offender, and, with its inherent personal accountability feature, also serves to deter potential abusers. In point of fact, the example given earlier to illustrate how one might populate the Countermeasure Matrix is exactly what did occur in thinking about PINs versus token-exchanging modems at CDI.

Figure 5 shows the results of intervention element #3 on the overall process. Before the intervention, single-tiered security options — options by and large *preventive* in nature — dominated both groups' thinking. After the intervention, methods that had a multi-tiered impact (“multi-tiered” was the terminology adopted by the security project team) were actively pursued. In the six months following the intervention, multi-tiered methods show distinct signs of being incorporated into planning processes of managers. During the several months immediately following the intervention, in fact, more multi-tiered than single-tiered options were being investigated.



**Figure 5. Effect of Intervention Element #3 on Pursuit of Multi-Tier Security Options**

What is revealing in this process is that the company did give careful consideration to methods that had a broader and longer term impact on security. Proposition 2, hence, receives support in this analysis.

A good indication of how knowledge of the Security Action Cycle had penetrated the security planning process was the following statement from a report in the seventh month:

*There was general agreement [among the firm's top managers] that the company needs to vigorously prosecute any one caught abusing the system. The deterrent impact of such highly publicized prosecutions could be significant.*

This statement certainly reflects the consensus that remedies such as prosecution should be considered, but even more importantly, that there will be a feedback impact from such actions and a deterrent effect on the front end of the cycle.

## Implications for Research and Practice

Evidence in favor of proposition 1 was found at both sites. In short, managers were generally not equally versed in all countermeasures in the Security Action Cycle. They tended to see computer security as a way to prevent losses and thereby mitigate further downstream damage. Much less frequently were they concerned about how to recover from a security breach or system loss and seek remedies. Moreover, managers were seldom attuned to deterrents as a tool for reducing system risk. They were even less aware of the value of systematic and purposeful detection. Hardly any participants demonstrated an awareness of the feedback effect of countermeasures.

Given that the present study examined proposition 1 in only two sites (albeit through a reasonable number of participants and documented instances in each site), researchers may want to test the generalizability of these findings more broadly. There are reasons to believe that the Security Action Cycle may be even less well known outside of North America (other than, possibly, Sweden), a circumstance which offers interesting cross-cultural research opportunities.

Proposition 2 also found support in the study. Awareness training, the security planning model, and Countermeasure Matrix appeared to have significantly influenced subsequent security planning, despite their, perhaps, more complex and intricate theoretical underpinnings. Researchers should investigate the long lasting effect of interventions such as the one reported here. It is possible, of course, that managers could lose this orientation and revert back to atheoretical approaches in addressing security issues.

Researchers should also test the viability of theory-based security planning in other contexts. Little scientific work has been done in this vein, and since deterrence theory has proven to be remarkably versatile in the computer security field in general (e.g., Harrington, 1997), there are many avenues in security planning to explore through this theory base. An open question, for example, is whether even a well thought-out program will lead to employees internalizing corporate security goals. Longitudinal research is perhaps best suited to examine a process such as this occurring over time. Field experiments, moreover, would allow us to conclude more definitively that theory-based tools produce more satisfactory outcomes. Additional action research or field studies could be very helpful in uncovering patterns of security planning and implementation. Using these and alternate techniques,

additional studies can also advance knowledge by confirming or disconfirming the Goodhue-Straub (1991) model of managerial concern.

New research opportunities are also suggested by this work. We need further studies in the general concept of risk in the computer security arena. The current work assumes a connection between increased planning and increased safeguards as well as the onward connection between increased safeguards and decreased risk. These assumptions may not be valid. Ironically, the downstream effects of security planning could create additional risks of their own, for instance. Adding security functionality to an existing system — IT or manual — does increase the complexity of the total system, which, in turn, might increase rather than decrease the total risk. Moreover, controls create more closely coupled systems; this also leads to increased risk of failure (Perrow, 1984).

From the standpoint of practice, if the responses of CDI and CPC managers represent a not untypical set of responses and if many managers, indeed, tend to be less informed about available measures to reduce systems risk, what can be done to alter both perceptions and knowledge? In particular, can knowledge of the full spectrum of security methods be conveyed so that it can be incorporated into managerial thinking? This study suggests that successful endeavors in this vein can build effective security from the planning stage onward and, hopefully, lower system risk.

Specifically, the results here indicate that managers are not aware of all of the security countermeasures available to them. Training and planning tools go hand-in-hand in proffering a means to change this situation. Moreover, in spite of the greater challenge posed by theoretically-oriented models, professionals will be well served by mastering and applying these principles to security planning. But implementers should be cautioned that one shot programs, just like short term management commitment, may have little long term impact (Banerjee, et al., 1998).

## Guidelines for Practice

Adopting the following steps and executing them well, managers can change the security environment in their organizations. Guidelines are presented in a capsulated form as Table 3; those that need further explication are enumerated briefly below.

<b>Phase</b>	<b>Guideline</b>	<b>Action plan</b>
Phase 1 - Recognition of security problem	<i>1.1. Gain top management support</i>	Educate top management about the Security Action Cycle and present them with obvious vulnerabilities and resources required to secure systems at some minimal “acceptable” level.
	<i>1.2. Adopt security risk planning model (SRP)</i>	Integrate SRP into the organization’s standard planning approach.
	<i>1.3. Institute security awareness program</i>	Offer optional security training; link mandatory training with new employee orientation and/or computer account issuance; teach participants the theoretical principles of the Security Action Cycle.
Phase 2. Risk analysis	<i>2.1. Carry out risk assessment program</i>	Determine unacceptable risks by organizing a wide-ranging risk program using teams of security officers and targeted users; evaluate existing systems, all new vendor products and IT projects; investigate security breaches.
Phase 3. Alternatives generation	<i>3.1. Consider options to deal with each risk</i>	Teams determine possible countermeasures for unacceptable risk by applying the security action cycle to each unacceptable risk
Phase 4. Planning decision	<i>4.1. Choose solutions</i>	Teams of security experts and targeted users develop countermeasures matrices for each unacceptable risk; determine security measures.
Feedback	<i>5.1. Disseminate information about security actions taken</i>	Initiate routine and exception security reporting practices, then communicate on a regular basis disciplinary actions regarding security to employees.

Table 3. Managerial Guidelines for Coping with Systems Risk

Guideline 1.2. Planning of security projects calls for a reasoned, general purpose methodology (von Solms et al., 1994), such as SRP. Other approaches are also viable (Luker, 1990), but the essential point is that some phased approach be utilized. To take action in this area, integrate a security risk approach with the organization’s regular IT planning (see also Baskerville, 1993).

Guideline 1.3. To heightened security awareness on the part of managers, professionals, technicians, contractors, etc., all relevant groups should be provided with sufficient training and supporting reference materials to allow them to properly protect and otherwise manage information assets. Training materials should communicate higher level concepts, such as the Security Action Cycle, but also detailed information about specific vulnerabilities and feasible responses in the organization's present setting. If the organization already has infosecurity policies, these should be reviewed with student-employees carefully during this training. If not, these should be created as a parallel activity and fed back into the system for subsequent rounds of training. For the greatest effectiveness, new employees should receive consciousness-raising and security awareness in their company orientation program while veteran employees should receive update and refresher programs.

Guideline 2.1. A prerequisite for devising a protection plan (Eloff, Labuschagne, and Badenhorst, 1993; DeMaio, 1995) and implementing security controls, risk analyses or comprehensive reviews of current security are usually carried out in organizations via teams of security officers and targeted users. Among the options for performing risk assessment, older techniques such as checklists and Courtney's probability risk analysis (1977) are still in use (Baskerville, 1993). New techniques such as threat tree analysis do not depend on exact probabilities to assess risk, but rather semantic matches to terms like "moderate," "low," and "high" (Weiss, 1991; Smith, 1989). This is one reason why threat tree analysis is recommended by the US Dept. of Defense (Department of Defense, 1988). The point of all of these techniques is to prioritize and then determine the level of risk that is "unacceptable" to the organization. If fifty systems risks are identified, an 80-20 pareto principle may suggest that the firm needs to seriously respond, for example, to only the first sixteen "unacceptable" risks.

Guideline 5.1. Feedback of various kinds is critical for creating a downstream deterrent effect on potential abusers. Managers should initiate routine and exception security reporting practices and then take further actions in this regard. Feedback actually consists of on-going dissemination of security actions taken and policies deployed and it should be more a part of corporate culture than a set of formal, one time exercises. Straub (1986b) and Hoffer and Straub (1994) identify several processes by which managers can communicate security information, values and goals to employees. Conventional departmental meetings and informal discussions are good ways in addition to formal training and

educational sessions. Unless suspects have been given due process in a court of law, no offender should be identified by name. Nonetheless, statements about disciplinary actions taken, such as reprimand or dismissal for violation of security policies, will provide the relevant feedback to potential abusers.

## **Conclusion**

No system can be made absolutely secure. In spite of this fact, it is possible to formalize parts of the security system that can be efficiently and effectively formalized, as we have seen. The advantage of such formalization is that it frees up other resources to be used to monitor those parts that cannot be formalized, or were selected not to be formalized. Thus, inadequate security in many organizations is a situation that can and should be remedied.

The present study provides evidence that practitioners are willing and able to adopt theory-based tools for security planning. The interview and action research findings offer empirical support for the propositions that measurable improvements can be made in these critical activities. While there is no doubt that many security consultants have excellent instincts with regard to what works and what does not, these empirical approaches help to raise the discussion above the level of folklore and into the realm of science. Additional work along these lines is very much needed, however.

## *References*

- ABA. "Report on Computer Crime," pamphlet, The Task Force on Computer Crime, American Bar Association, Section on Criminal Justice, 1984.
- AICPA. "Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries," pamphlet, American Institute of Certified Public Accountants, Inc., 1211 Ave. of the Americas, NY, NY, 1984.
- Arnum, E. "Doing Business on the Internet - A Question of Balance," *Business Communications Review* (25:8, August), 1995, pp. 35-38.
- Badenhorst, K.P. and Eloff, J.H.P. "Framework of a Methodology for the Life Cycle of Computer Security in an Organization," *Computers & Security* (8:5, August), 1989, pp. 433-442.
- Ball, L. and Harris, R. "SMIS Member: A Membership Analysis," *MIS Quarterly* (6:1, March), 1982, pp. 19-38.
- Banerjee, D., Cronan, T.P. and Jones, T.W. "Modeling IT Ethics: A Study in Situational Ethics," *MIS Quarterly* (forthcoming), 1998.
- Baskerville, R. *Designing Information Systems Security*, John Wiley, Chichester, UK, 1988.
- Baskerville, R. "Risk Analysis as a Source of Professional Knowledge," *Computers & Security* (10:8, December), 1991, pp. 749-764.
- Baskerville, R. "An Analytical Survey of Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Computing Surveys* (25:4, December), 1993, pp. 375-414.
- Baskerville, et al. Comparison of action research now being conducted, In press.***
- Blumstein, A. "Introduction," In *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*, A. Blumstein, J. Cohen and D. Nagin (Ed.), National Academy of Sciences, Washington, DC, 1978.
- Brancheau, J.C., Janz, B.D. and Wetherbe, J.C. "Key Issues in Information Systems Management: 1994-95 SIM Delphi Results," *MIS Quarterly* (20:2, June), 1996, pp. 225-242.
- Brancheau, J. and Wetherbe, J.C. "Key Issues in Information Systems: 1986," *MIS Quarterly* (11:1, March), 1987, pp. 23-45.

- Brown, R.O. "What You Need to Know to Plan for Disaster," *Networking Management*, (11:4, April), 1993, pp. 25-27.
- Burger, K. "The New Age of Anxiety," *Insurance & Technology* (18:10, October), 1993, pp. 48-54.
- Carroll, J. *Computer Security*, Butterworths, Boston, 1987.
- Colton, K.W., Tien, J.M., Davis, S.T., Dunn, B. and Barnett, A.I. *Computer Crime: Electronic Fund Transfer Systems and Crime*, U.S. Department of Justice, Bureau of Justice Statistics, Washington, DC, 1982a.
- Cook, T.D. and Campbell, D.T. *Quasi Experimentation: Design and Analytical Issues for Field Settings*, Rand McNally, Chicago, 1979.
- Colton, K.W., Tien, J.M., Davis, S.T., Dunn, B. and Barnett, A.I. "Electronic Funds Transfer Systems and Crime," supported by Grant No. 80-BJ-CX-0026, U.S. Bureau of Justice Statistics. Referenced by special permission.
- Courtney, R. "Security Risk Assessment in Electronic Data Processing," *AFIPS Conference Proceedings of the National Computer Conference 46*, Arlington, VA, 1977, pp. 97-104.
- Davies, J.R. and Warman, A. "Computer Fraud: Has Management Lost Control? (Part 1)," *Management Accounting-London* (70:7, July-August), 1992, pp. 34-35.
- de Koning, W.F. "A Methodology for the Design of Security Plans," *Computers & Security* (14:7), 1995, pp. 633-643.
- DeMaio, H.B. "Protecting and Controlling Information in Complex System Environments," In *Handbook of IS Management, 1994-95 Yearbook*, R. Lumbaugh (Ed.), Supplement to 3rd Edition, Auerbach, New York, 1995, pp. S-281-294.
- Denning, P. "The Internet Worm," In *Computers Under Attack: Intruders, Worms and Viruses*, P. Denning (Ed.), Addison-Wesley, Reading, MA, USA, 1990, pp. 193-200.
- Department of Defense. "System Security Engineering Program Management Requirements," MIL-STD-1785, June 20, 1988.
- Dickson, G.W., Leitheiser, R.L., Wetherbe, J.C. and Nechis, M. "Key Information Systems Issues for the 80's," *MIS Quarterly* (8:3, September), 1984, pp. 135-159.
- Dixon, R., Marston, C. and Collier, P. "Report on the Joint CIMA and IIA Computer Fraud Survey," *Computers & Security* (11:4, July), 1992, pp. 307-313.

- Ehrlich, L. "Participation in Illegitimate Activities: A Theoretical and Empirical Investigation," *Journal of Political Economy* (81), 1973, pp. 521-564.
- Eloff, J.H.P., Labuschagne, L. and Badenhorst, K.P. "A Comparative Framework for Risk Analysis Methods," *Computers & Security* (12:6, October), 1993, pp. 597-603.
- Farquhar, Bill, "One Approach to Risk Assessment," *Computers & Security*, 10, 1 (February), (1991), 21-23.
- Fielding, N. and Fielding, J. *Linking Data*, Sage, Newbury Park, CA, 1986.
- Fisher, R. *Information Systems Security*, Prentice-Hall, Englewood Cliffs, NJ, 1984.
- Flanagan, W.G. and McMenemy, B. "The Playground Bullies are Learning How to Type," *Forbes*, 21 February 1992, pp. 184-189.
- Forcht, K. "Bolstering Your Computer's Immune System," *Security Management* (36:9, September), 1992, pp. 134-140.
- Forcht, K.A. *Computer Security Management*, Boyd & Fraser, Danvers, MA, 1994.
- Fromkin, H.L. and Streufert, S. "Laboratory Experimentation," In *Handbook of Industrial and Organizational Psychology*, Rand McNally Publishing Company, Inc., Chicago, IL, 1976, pp. 415-465.
- Gips, M. "Tales of Woe," *Security Management* (39:5, May), 1995, pp. 10.
- Goodhue, D.L. and Straub, D.W. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures," *Information & Management* (20:1, January), 1991, pp. 13-27.
- Gopal, R. and Sanders, G.L. "The Effect of Preventive and Deterrent Software Piracy Strategies on Producer Profits," *Proceedings of the Thirteenth International Conference on Information Systems (ICIS)*, Dallas, TX, USA, 1992, pp. 161-170.
- Gopal, Ram D. and G. Lawrence Sanders, "Preventive and Deterrent Controls for Software Piracy," *Journal of Management Information Systems: JMIS* (3: 4, Spring), 1997, pp. 29-47.
- Harrington, S.J. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3, September), 1996, pp. 257-258.
- Hartlog, C. and Herbert, M. "1985 Opinion Survey of MIS Managers: Key Issues," *MIS Quarterly*, (10:4, December), 1986, pp. 351-361.

- Hoffer, J.A. and Straub, D.W. "The 9 to 5 Underground: Are You Policing Computer Crimes?," *Sloan Management Review* (30:4, Summer), 1989, pp. 35-44.
- Hoffman, L.J. "Risk Analysis and Computer Security: Towards a Theory at Last," *Computers & Security* (8:1, February), 1989, pp. 23-24.
- Jenkins, A.M. "Research Methodologies and MIS Research," In *Research Methods In Information Systems*, E. Mumford, R. A. Hirschheim, G. Fitzgerald and A. T. Wood-Harper (Ed.), North Holland, Amsterdam, 1985, pp. 103-117.
- Hsaio, D.K., Kerr, D.S. and Madnick, S.E. *Computer Security*, Academic Press, New York, 1979.
- Kearns, J. "Users Blase, Study Reveals," *Computing Canada*, (20:1), January 5, 1994, pp. 28.
- Keil, M. "Pulling the Plug: Software Project Management and the Problem of Project Escalation," *MIS Quarterly* (19:4, December), 1995, pp. 421-447.
- King, J. "Survey Finds Computer Fraud Often an Inside Job," *Computerworld*, (29:12), March 20, 1995, pp. 16.
- King, W.R. "Evaluating the Effectiveness of Your Planning," *Managerial Planning* (33:5), 1984, pp. 4-8, 26.
- Kusserow, R.P. "Computer-Related Fraud and Abuse in Government Agencies," bound report, U.S. Dept. of Health and Human Services, 1983.
- Lederer, A.L. and Sethi, V. "Critical Dimensions of Strategic Information Systems Planning," *Decision Sciences* (22:1, Winter), 1991, pp. 104-119.
- Local Government Audit Inspectorate "Computer Fraud Survey," Department of the Environment, 1981.
- Loch, K.D., Houston H. Carr and Warkentin, M.E. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (17:2), 1992, pp. 173-186.
- Luker, N.W. "Do You Trust Your Employees?," *Security Management* (34:9, September), 1990, pp. 127-130.
- Martin, J. *Security, Accuracy, and Privacy in Computer Systems*, Prentice-Hall, Englewood Cliffs, NJ, 1973.
- McLean, E.R. and Soden, J.V. *Strategic Planning for MIS*, John Wiley, New York, 1977.

- Nance, W.D. and Straub, D.W. "An Investigation into the Use and Usefulness of Security Software in Detecting Computer Abuse," *Proceedings of the 9th International Conference on Information Systems (ICIS)*, Minneapolis, MN, USA, 1988, pp. 283-294.
- Neumann, P.G. "Inside Risks," *Communications of the ACM*, (37:5), 1994, pp. 146.
- Niederman, F., Brancheau, J.C. and Wetherbe, J.C. "Information Systems Management Issues for the 1990s," *MIS Quarterly* (15:4, December), 1991, pp. 475-495.
- Panettieri, J.C. "InformationWeek/Ernst & Young Security Survey," *InformationWeek*, (27 November 1995).
- Parker, D.B. *Computer Security Management*, Reston, Reston, VA, 1981.
- Parker, D.B. *Fighting Computer Crime*, Scribner's, New York, 1983.
- Peach, S. "Disaster Recovery: An Unnecessary Cost Burden or an Essential Feature of Any DP Installation?," *Computers & Security* (10:6, October), 1991, pp. 565-568.
- Pearson, F.S. and Weiner, N.A. "Toward an Integration of Criminological Theories," *Journal of Crime and Criminology* (76:1, Winter), 1985, pp. 116-150.
- Perrow, C. *Normal Accidents: Living with High-Risk Technologies*, Basic Books, New York, 1984.
- Ramanujam, V. and Venkatraman, N. "Planning System Characteristics and Planning Effectiveness," *Strategic Management Journal* (8:5), 1987, pp. 453-468.
- Schein, E.H. *The Clinical Perspective in Fieldwork*, Sage Publications, Newbury Park, CA, 1987.
- Schwartz, M. "Computer Security: Planning to Protect Corporate Assets," *Journal of Business Strategy* (11:1, January-February), 1990, pp. 38-41.
- Senge, P. *The Fifth Discipline*, Doubleday, New York, 1990.
- Simon, H. *The New Science of Management Decision*, Harper and Brothers, New York, 1960.
- Smith, S. "LAVA's Dynamic Tree Analysis," *Proceedings of the 12th National Computer Security Conference*, 1989.
- Spafford, E. "The Internet Worm: Crisis and Aftermath," *Communications of the ACM* (32:6, June), 1989, pp. 678-687.

- Steiner, G.A. *Strategic Planning: What Every Manager Must Know*, New York Free Press, New York, 1979.
- Steiner, G.A. "Evaluating Your Strategic Planning System," In *Implementation of Strategic Planning*, P. Lorange (Ed.), Englewood Cliffs, NJ, Englewood Cliffs, NJ, 1982.
- Stone, E. *Research Methods in Organizational Behavior*, Goodyear Publishing Company, Inc., Santa Monica, CA, 1978.
- Straub, D.W. "Computer Abuse and Computer Security: Update on an Empirical Study," *Security, Audit, and Control Review* (4:2, Spring), 1986a, pp. 21-31.
- Straub, D.W. "Deterring Computer Abuse: the Effectiveness of Deterrent Countermeasures in the Computer Security Environment," unpublished dissertation, Indiana University Graduate School of Business, 1986b.
- Straub, D.W. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), 1990, pp. 255-276.
- Straub, D.W., Carlson, P.J. and Jones, E.H. "Deterring Highly Motivated Computer Abusers: A Field Experiment in Computer Security," In *IT Security: The Need for International Cooperation*, G. G. Gable and W. J. Caelli (Ed.), North-Holland, Amsterdam, 1992, pp. 309-324.
- Straub, D.W., Carlson, P.J. and Jones, E.H. "Deterring Cheating by Student Programmers: A Field Experiment in Computer Security," *Journal of Management Systems* (5:1), 1993, pp. 33-48.
- Straub, D.W. and Nance, W.D. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1, March), 1990, pp. 45-62.
- Straub, D.W. and Widom, C.S. "Deviancy by Bits and Bytes: Computer Abusers and Control Measures," In *Computer Security: A Global Challenge*, J. H. Finch and E. G. Dougall (Ed.), Elsevier Science Publishers B.V. (North Holland), Amsterdam, 1984, pp. 431-442.
- Vandaele, W. "Participation in Illegitimate Activities: Ehrlich Revisited," In *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*, A. Blumstein, J. Cohen and D. Nagin (Ed.), National Academy of Sciences, Washington, D.C., 1978.
- Venkatraman, N. "Research on MIS Planning: Some Guidelines from Strategic Planning Research," *Journal of Management Information Systems* (2:3, Winter), 1985-86, pp. 65-77.
- von Solms, R., van de Haar, H., von Solms, S.H. and Caelli, W.J. "A Framework for Information Security Evaluation," *Information & Management* (26:3, March), 1994, pp. 143-153.

Weiss, J. "A System Security Engineering Process," *Proceedings of the 14th National Computer Security Conference*, 1991.

Wood, C.C. "A Context for Information Systems Security Planning," *Computers & Security* (7:5, October), 1988, pp. 455-465.

Yin, R.K. *Case Study Research: Design and Methods*, Sage Publications, Thousand Oaks, CA, 1994.

## APPENDIX

<p><b>Computer Security Policy/Risk Project Security Views Interview Script</b></p>
---------------------------------------------------------------------------------------------

Name of interviewee: \_\_\_\_\_

Name of liaison: \_\_\_\_\_

Name(s) of interviewer(s): \_\_\_\_\_

Date/time of interview: \_\_\_\_\_  
interview: \_\_\_\_\_

Length of

<p><b>Section I. Warm-Up Questions</b></p>
--------------------------------------------

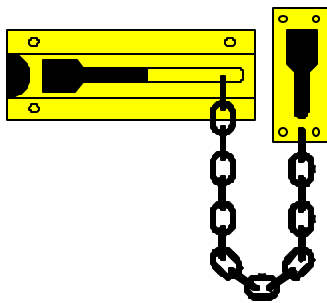
1. How long have you been with the company?
2. Did you work elsewhere before joining the company? If yes, how long were you there and what positions did you hold?
3. What is your current position (role) in the organization? **[The interviewee may answer this question simply with their title. Probe even if the title does seem to make the interviewee's role obvious. A follow-on question such as "Exactly what do you do in this job?" may suffice, but if not, ask some additional questions. We need an elaboration of their role in order to understand the current organizational structure, with respect to security, and how this structure as it currently exists will be able to adapt to the need to secure the new systems coming on line. A secondary use of this qualitative data will be to assess the overall security personnel structure in order to make recommendations for the implementation and roll-out.]**
4. How long have you had this position?
5. To whom do you report?

<p><b>Section II. Characterization of Firm</b></p>
----------------------------------------------------

I would like to hear your views on the firm itself, its culture, its character, its idiosyncrasies, and so forth? What is it like working here? What is the “spirit” of the organization? **(This is a question trying to get at culture of the organization.)**

In your view, what is the purpose, mission, or driving force behind the firm? What does it have to do right to continue to be prosperous, successful, and competitive?

### **Section III. General Opinions and Views about Security at the Firm**



Next are questions related to your views or opinions about the protection of the company’s computerized information systems in general. When you are asked in the interview about your views on some scenarios, for example, you can consider every kind of computerized information system in the company, even PCs and workstations.

### **Scenario A: “Worst Possible Thing that Could Happen” Security Incident**

Please think about the broad outlines of the security “incident” described in the following scenario, ponder some questions we are going to ask you, and then give use your answers.

**[Interviewer should hand the interviewee a boldface, large font printed version of the following scenario--the material within quotation marks--to help them answer questions about the two scenarios following.]**

“This firm has experienced a security ‘incident’ in which data, records, files, programs, or computer hardware have been improperly and deliberately used, modified, destroyed, stolen, or damaged. The incident is either internal--that is, originating inside the organization--or external in origin.

The incident has resulted in one or more of the following losses:

- (1) financial losses, either unbudgeted expenses, loss of revenues, loss of clients, and/or other direct actual dollar losses,**

- (2) opportunity losses or costs,
- (3) legal liabilities,
- (4) severe embarrassment from media exposure of the incident.”

## Questions

2a. What is the worst thing that you could possibly imagine happening here at the company that would fit this general description? Focus on the dire consequences of this scenario more than on how likely it is to occur. In other words, don't worry if the incident you imagine is not very likely to ever occur!!!

Can you give me as many details as occur to you?

**[Interviewer should probe for as many statements by the interviewee as possible. Through this question we are trying to get as much qualitative data as possible about the company culture --what is valued most (and, therefore, what should be protected most) and what are the management decision-making drivers.]**

2b. What do you think might be the underlying factors that would explain how such an incident could have occurred?

**[Interviewer should probe for as many details as possible. Through this question we are trying to get as much information as possible about general or high level security vulnerabilities that the policy and the detailed risk assessment will need to address.]**

## **Scenario B: Most Likely Security Incident that Could Happen”**

Please think about the broad outlines of the security “incident” described in the following scenario, ponder some questions we are going to ask you, and then give use your answers.

“The firm has experienced a security ‘incident’ in which data, records, files, programs, or computer hardware have been improperly and deliberately used, modified, destroyed, stolen, or damaged. The incident is either internal--that is, originating inside the organization--or external in origin.

The incident has resulted in one or more of the following losses:

- (1) financial losses, either unbudgeted expenses, loss of revenues, loss of clients, and/or other direct actual dollar losses,**
- (2) opportunity losses or costs,**
- (3) legal liabilities,**
- (4) severe embarrassment from media exposure of the incident.”**

## **Questions**

- 3a. What is the worst thing that is likely to happen here at the firm that would fit this general description? This time, please focus on a serious incident that you think is likely to occur. In other words, don't worry if the incident you imagine is not the most serious incident you can think of!!! Focus on what seems to be the most vulnerable security asset.

Can you give me as many details as occur to you?

**[Interviewer should probe for as many statements by the interviewee as possible. Through this question we are trying to get as much qualitative data as possible about the high level vulnerabilities that will inform our risk analysis. We are looking for and should probe --without leading the witness--for statements like: “Most people are not very concerned about backing up their personal computers and I’ve seen a lot of wasted work restoring systems from scratch as a result. I back my own system up once a day now.” ]**

- 3b. What do you think might be the underlying factors that would explain how such an incident could have occurred?

**[Interviewer should probe for as many details as possible. Through this question we are trying to get as much information as possible about general or high level security vulnerabilities that the policy and the detailed risk assessment will need to address.]**

4. If you were asked to plan for some new security measures at the company, how would you go about doing this? Are there certain stages or phases that might be involved in your planning for improved security?

**[Interviewer should probe for as many statements by the interviewee as possible. Through this question we are trying to get as much qualitative data as possible about the company culture, especially such aspects as resistance to change and how seriously do employees think they should take security. The more individuals dwell on the complexities of deriving a security plan, the more aware they may be of the difficulties involved in designing and implementing security. A secondary research objective is to content-analyze for indications that individuals have or do not have a grasp of the embedded phases of deterrence, prevention, detection, recovery, and organizational response.]**

5. If a serious computer security incident occurred in an area you have some responsibility for, what are the steps you think would have to be taken to deal with the situation? Even if you feel that the entire matter should be turned over to the professionals inside and outside of the company, what steps should be taken?

**[Interviewer should probe for as many statements by the interviewee as possible. Through this question we are trying to get as much qualitative data as possible about the company culture, especially such aspects as resistance to change and how seriously do employees think they should take security. The more individuals dwell on the complexities of deriving a security plan, the more aware they may be of the difficulties involved in designing and implementing security. A secondary research objective is to content-analyze for indications that individuals have or do not have a grasp of the embedded phases of deterrence, prevention, detection, recovery, organizational response, organizational learning and feedback.]**

<p style="text-align: center;"><b>Security Breaches/Lapses in Security Incident #1</b></p>
------------------------------------------------------------------------------------------------

6. Are you aware of any incidents that have occurred over the last 5 years in the security of information systems here at the firm? We are interested in the whole range of incidents involving the protection of the information resource. Viruses would qualify, as would a deliberate act of computer abuse or computer crime. Loss of data from a lightning strike is equally useful information. What ever you can think of would be helpful. **[Probe for both intentional security breaches and lapses in procedure (backup procedures, for example) that have resulted in losses to the company. ]**
- 6a. Description of incident: (What are the facts of the incident? Where relevant, assets attacked; method used; perpetrator, if known)
- 6b. What losses occurred? **[Direct the interviewee's attention to the generic scenario for a listing of some of the losses that can occur.]**
- 6c. How was the incident discovered?

**[Probe for the presence of systems controls alerting someone that there was a problem. If discovery was accidental, probe for the actions that led to the discovery.]**

- 6d. How was the incident handled from an administrative point of view?

**[Probe for the extent to which perpetrators were disciplined or not. Ask follow-up questions to gather information about the presence or absence of formal recovery procedures, adjudication of the incident, and feedback to other employees about the problem.]**

<p style="text-align: center;"><b>Security Breaches/Lapses in Security Incident #2</b></p>
------------------------------------------------------------------------------------------------

**6.** Are you aware of any incidents that have occurred over the last 5 years in the security of information systems here at the firm? We are interested in the whole range of incidents involving the protection of the information resource. Viruses would qualify, as would a deliberate act of computer abuse or computer crime. Loss of data from a lightning strike is equally useful information. What ever you can think of would be helpful. **[Probe for both intentional security breaches and lapses in procedure (backup procedures, for example) that have resulted in losses to the company. ]**

**6a.** Description of incident: (What are the facts of the incident? Where relevant, assets attacked; method used; perpetrator, if known)

**6b.** What losses occurred? **[Direct the interviewee's attention to the generic scenario for a listing of some of the losses that can occur.]**

**6c.** How was the incident discovered?

**[Probe for the presence of systems controls alerting someone that there was a problem. If discovery was accidental, probe for the actions that led to the discovery.]**

**6d.** How was the incident handled from an administrative point of view?

**[Probe for the extent to which perpetrators were disciplined or not. Ask follow-up questions to gather information about the presence or absence of formal recovery procedures, adjudication of the incident, and feedback to other employees about the problem.]**

## *Endnotes*