Coping With Systems Risk: Security Planning Models for Management Decision Making[1]

By: Detmar W. Straub
Department of Computer Information Systems
College of Business Administration
Georgia State University
Atlanta, GA 30302-4015
U.S.A.
dstraub@gsu.edu

Richard J. Welke
Department of Computer Information Systems
College of Business Administration
Georgia State University
Atlanta, GA 30302-4015
U.S.A.
rwelke@gsu.edu

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.*

Keywords: Information security planning, systems security risk, security awareness training, action research

ISRL Categories: EF01, EF01.UF, EF02, EF03, EK, EK01, EK01.UF, EK03, EK08, EK10

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 to 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, the model of managerial decision making (Simon 1960) offers direction as to generic stages in an effective planning approach.

[1]Robert Zmud was the accepting senior editor for this paper.

studies (Loch et al. 1992 ; Straub 1986a, 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 adopted to reduce systems risk, fall into four distinct, sequential activities, namely: (1) deterrence, (2) prevention, (3) detection, and (4) recovery (Forcht 1994; Martin 1973; Parker 1981;). 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 antisocial personalities, the theory is well established in criminology (Blumstein 1978; Pearson and Weiner 1985). It posits that individuals with an instrumental intent to commit antisocial 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 a certainty of getting caught and punished severely.

General deterrence theory has been applied successfully to the IS environment by Straub and his research partners (Hoffer and Straub 1989; Straub 1990; Straub and Nance 1990; Straub et al. 1992; 1993). 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, the work 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 the activities of managers and 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 interrelationships, 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 antisocial 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).

When potential abusers choose to ignore deterrents, the next line of system defense is *preventives*, such as locks on computer room doors and password access controls.

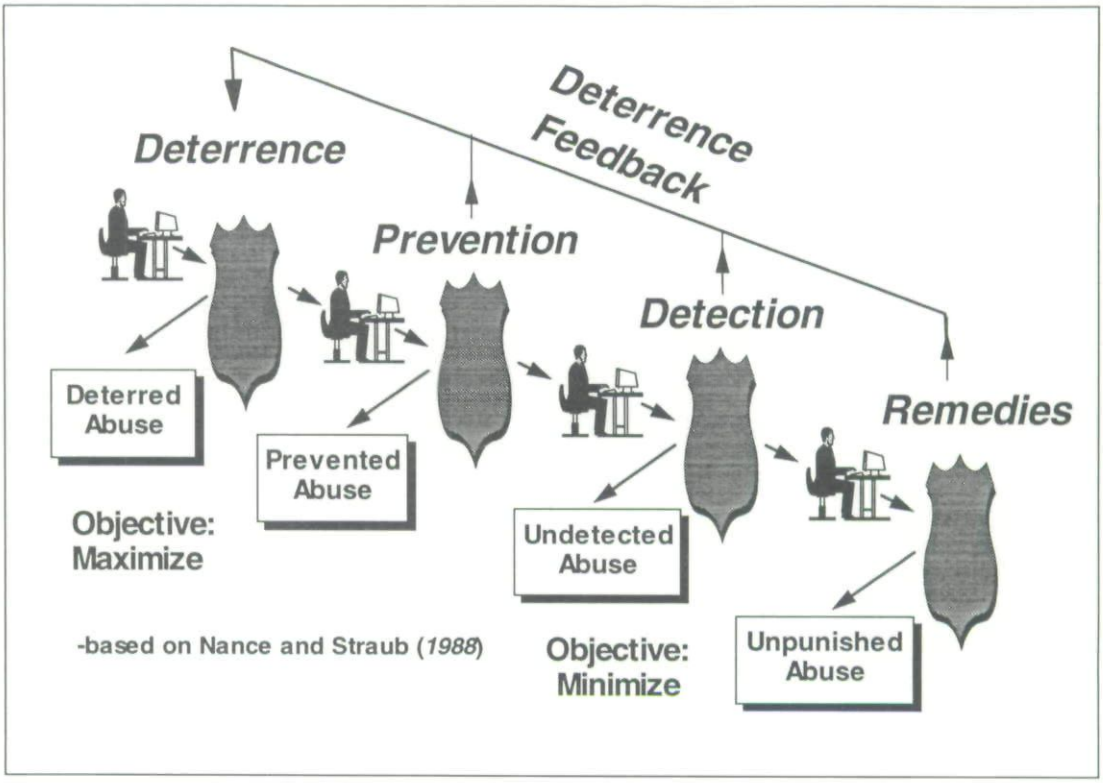

Figure 2. The Security Action Cycle

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. Another example would be a virus scanning report. 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 (Hoffer and Straub 1989; Straub and Nance 1990) 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 for the effectiveness of these techniques in practice 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. 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 managers' 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, the following two propositions were studied:

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.

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