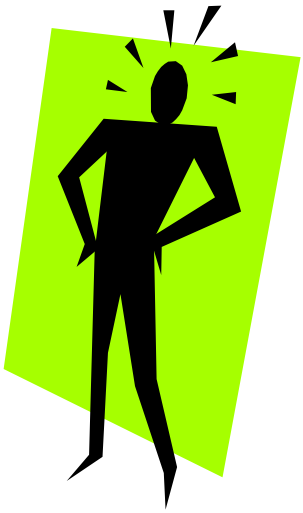
9.1 Make a Commitment to Protect Computer Data and the Business: Establishing a Good Control Environment

Any plan to protect computer data and the business has to start at the top. Management's commitment and attitude toward controls is the foundation of an effective computer and data protection system. Computer security and business continuity planning will not happen unless it is made a priority with the commitment of company resources.

Management's philosophy and actions must instill a control consciousness in employees throughout the organization. Security over company computer networks will fail without the integrity, ethical values, and competence of the people who create, administer, and monitor it. A strong computer security consciousness encouraged by management can improve the chances of meeting company objectives.

The control environment as set forth by management provides an atmosphere for people and computers to operate. A good control environment is not based on one procedure or circumstance, but a series of actions that permeate the organization's activities. Management needs to make clear the close linkage between people's duties and the way they are carried out. As appropriate, conduct investigations of computer crimes and discipline workers for security violations.



Create an organizational structure and work ethic that demonstrates management's commitment to information security. Establish a set of policies and procedures to clearly communicate both direction and management support. Train employees and ensure that control mechanisms are in place to address the risks faced by the company. Management will have a profound impact on security by mandating policies, controls, and proper training to address computer protection needs.

Management can effectively communicate computer policy and business objectives through impromptu discussions, group meetings, written memos, employee training sessions, and formal policies and procedures. Heighten security awareness by proposing hard questions to managers and employees. It's the process of the inquiry that sends the message and creates a moral climate. Management must be a role model by following security policies in appearance and in fact. All personnel must get a clear message from top management that computer protection and security is taken seriously.

Don't just give it lip service. Think in terms of the owners, stockholders, and other stakeholders who have an economic interest in the viability of the company. Start by making a reasonable investment of time and company resources to get the process going.