Managing Computer Security Risks

In today=s society, the protection of computers, computer data, and software programming has spawned a unique set of risks. In fact, liability and litigation continue to arise from misuse and abuse of computer systems, data bases, bulletin boards, e-mail, instant messaging, web pages, electronic funds transfer systems, and proprietary computer programs and from absent or ineffective disaster recovery procedures and data archiving. Protecting computers and information has become both a necessary business practice and a legal requirement. Anything short of adequate protection could result in a negligent act, a breach of privacy, or an infringement of intellectual property rights, possibly leading to tort, statute, and regulatory liabilities that can be attached to the organization, its directors and officers, managers, employees, and agents. Real estate management companies and property managers who rely on computers to maintain resident and tenant records as well as management information are likewise vulnerable.

Corporations today are faced with lessened standards of criminal liability and a trend to criminalize regulations that were once essentially civil. Federal legislation initially intended to fight criminal racketeering and narcotics-related crimes has given prosecutors broad powers to indict, compel plea bargaining, and force cooperation of individual or corporate defendants. Prosecution used to hinge on the concept of intent, but this has often been replaced by evidence of Awillful blindness,@ Arecklessness,@ Afailure to perceive (a risk),@ or Acollective knowledge@ for corporate liability. Added to this could be the expensive prospect of collateral prosecution and litigation or being twice charged, tried, and possibly fined or sentenced for a single violation. Although legal costs can be exorbitant, litigation also can damage a company=s

reputation; harm employee, customer, and investor relations; and possibly diminish credit lines.

Risk Awareness

How does one foresee a risk? It is hard to foresee a very specific risk; what matters in law is not that one be clairvoyant, but that one be aware of those risks that might affect one=s customers and that one takes appropriate precautions to alleviate those risks. This, in short, is a definition of the *duty of care.* But what should be your level of Aknowing?@ (Or, what should a reasonable person have known)? And what are the appropriate set of precautions? (Or, how much security should you have)?

Courts often evaluate foreseeability in terms of prior similar incidents and the circumstances surrounding the incident. This implies that you should be aware of prior incidents, and for computer systems, at several levelsCglobal, local, and site specific. Let us look at awareness levels:

*Global*CAn example would be a study on virus or hacker attacks. At the national level, there are crime surveys by the U.S. Census Bureau, the FBI, and the National Criminal Justice Reference Center. Many of the computer security trade journals will headline such studies.

*Local*CForecasting techniques have made accurate crime projections for city blocks, census tracts, and zip codes. There are companies that produce color-coded maps depicting crime vulnerability for any location in the United States. In addition, local police department crime statistics are available to the public.

*Site specific*CRisk assessments and security evaluations can be gathered from in-house loss

reporting, security surveys, vulnerability analyses, computer system penetration tests, and internal audits.

All of these can be used to determine the foreseeability of wrongful acts; you can argue that the degree of security should be directly proportionate.

A basic legal duty of corporate directors and officers is to be informed about company operations and not make poorly considered decisions or be negligent.

Reducing or Eliminating Vulnerability

The search for safeguards to recommend for reducing or eliminating the vulnerabilities in computer systems is endless. However, using the eleven steps outlined below that correspond to the functions of security will be key.

1. *Avoidance*—Before you consider controls, attempt to remove the threat or information subject to the threat.
2. *Deterrence*—Stop people from developing the intent to misbehave.
3. *Prevention*—Stop a harmful incident from occurring, give alarm, and record it.
4. *Detection*—Observe or discover an anomaly, give alarm, and record it.
5. *Mitigation*—Stop an attack, give alarm, record it, and minimize or prevent a loss.
6. *Transference*—Assign the appropriate parties to deal with an incident.
7. *Investigation*—Find the causes and failures and the guilty party.

8. *Sanction or credit*—Punish and reward the appropriate parties.
9. *Recovery*—Restore or compensate for the loss.
10. *Correction*—Implement or improve on the actions in steps 1 through 9 as needed to prevent a reoccurrence.
11. *Education*—Document and learn from the experience of the incident.

You can *avoid* a vulnerability by removing the threat from the information or other threatened asset or by removing the information from the threat. Examples include removing a disgruntled employee from a sensitive assignment or taking sensitive information away from him or her, thereby removing the means of misbehaving.

Deterrence is defined as discouraging from acting by fear or consideration of dangerous, difficult, or unpleasant attendant circumstances or consequences. *Fear* is the operative word here, and you can use it to great advantage for security.

Prevention is never totally possible; however, utilization of techniques such as signage, contracts of agreement or nondisclosure, compartmentalization of information, and security access systems for tracking movement of personnel and information, may make prevention a valuable tool for your organization.

Detection can be quite complex, as well as powerful, in its application. This is particularly true in computers, where automated detection can be effectively, comprehensively, and inexpensively achieved. The effect is to transfer detection to a human for response. In many cases in automated systems, informing an officer or administrator is insufficient to accomplish any of the other functions such as *mitigation,* and automatic triggering of another automated control is necessary.

Some of the remaining functions are mainly under management=s ultimate responsibility, along with the information owners, who may delegate their accountability to others. In large organizations, qualified security staffs often *investigate* crimes with the assistance of information security specialists. Otherwise, investigative firms are contracted for this specialized work.

Sanctions against perpetrators and those accountable for negligence are a management prerogative, although the information security department may serve as behind-the-scenes advisors. Management is also responsible for *rewarding* staff members who perform exemplary service in any of the functions relative to a loss incident.

Transference, recovery, and correction are the next three safeguard functions. *Transfer* of accountability usually means purchasing insurance coverage or self-insuring, which is done by risk managers who specialize in insurance. Computer crime insurance and all-risk information insurance are becoming popular. *Recovery* from physical disasters is performed by information systems recovery experts in the information security department or by a specialist group. Otherwise, recovery is accomplished by restoring that which was lost or accepting and adapting to the consequences. *Correction* consists of updating and restoring information security after a loss incident to minimize the possibility of a repeat of the loss.

Finally, you can *educate* stakeholders by fully documenting any losses that occur and publishing the results appropriately or using the documentation for training purposes. Documenting losses is important for justifying future budgets and security plans. You should keep a file of cases within the organization, as well as cases reported outside, which are useful to apply as examples of threats and vulnerabilities for future security purposes.