Implementing Computer Security: If Not Now, When?

M. E. Kabay, PhD, CISSP

Security Leader, INFOSEC Group, AtomicTangerine, Inc.

Security is increasingly recognized as a necessity in today's highly competitive environment. The trouble is that in practice, corporate security policies too often pay only lip service to protecting data assets; in one security analysis in my own practice, a corporate security policy consisted solely of the statement, "The Company recognizes the importance of security in its operations."

Arguments About Security

- The traditional excuses for leaving security until an unspecified "later" time include
- We're just a widget manufacturer; who would care about harming or seeing our data?
- It's never happened here in all the years we've been working.
- Security is a pain in the... uh... neck; that is, it interferes with productivity.
- Fundamentally, it costs too much.
- These objections are weak. Let's take them in turn.

Vulnerability: Regardless of how uninteresting your data appear, they are still required for the continued operation of your organization; else why include them in computers and networks? Security involves not only protection against deliberate attack by disgruntled or dishonest employees or contractors, and sociopathic criminal hackers, but also against errors and omissions and acts of God such as fires and floods. Legally and morally, managers must protect the interests of stakeholders: owners, shareholders, employees, clients and others who depend on the organization for their livelihood or quality of life. Failing to do so may put managers at risk of lawsuits and even of criminal prosecution.

History: The past is at best an uncertain guide to the future. A company that is at the leading edge of its industry is at greater risk of industrial espionage and sabotage than a mediocre player in its field. And failing to protect assets is an invitation to attack by the unscrupulous.

Interference: Security is especially irritating when it is imposed on others without consultation. Effective implementation demands thoroughgoing collegiality and involvement of everyone in the organization. Security policies will fail if upper management are seen to skirt the requirements they attempt to impose on other employees.

Cost: One cannot measure the value of security simply by measuring short-term costs. Prudent managers accept their obligation to provide for insurance as part of their operating costs; most people also pay for maintenance and support contracts on their computer hardware and software. Security precautions are just another component of organizational strategy for avoiding catastrophic losses. In addition, in today's electronic marketplace, good security is essential for market development. Instead of viewing security as a black hole of expense, wise marketers are seeing security as a tool for value creation.

Key Issues for Today's Security

There are several areas demanding increased attention in today's computing environment.

One of the success stories in network architecture is the near ubiquity of LANs and WANs. Enormous amounts of information are being transmitted within organizations and among difference campuses using high-speed networks. Managers should ensure that all such traffic is encrypted to prevent eavesdropping. Common tools of information warfare such as network sniffer programs (which capture packets by putting workstations into "promiscuous" mode) are defeated by encryption.

Longer-range transmissions through the Internet should also be protected by encryption. For commercial use (i.e., not personal use), ViaCrypt PGP is highly regarded for both encryption and digital signature. PGP can be used legally by businesses in the U.S. and Canada only. However, even though export of PGP is banned by the U.S. government's International Traffic in Arms Regulations, there is no restriction on sending and receiving encrypted messages. In countries where encryption is allowed, foreign correspondents can therefore send and receive PGP encrypted messages without risk. Other, weaker encryption schemes have received export permits from the U.S. government and can also be used for reasonably safe communications through the Internet.

Identification and authentication are problems which will grow in importance as more people join the information age. The historical emphasis on "what you know" is shifting among information security professionals to depending on "what you have" as well as "what you are/do". Token-based authentication provides a randomly-generated password that expires within a minute or two and unambiguously identifies the smart card which generated it. Unless users lose their assigned smart card, no one else can masquerade as them when logging into a network. The strength of such smart cards provides protection of information in the network; in combination with digital signatures, it also provides non-repudiation. That is, a user who has not reported a lost smart card cannot plausibly deny that they sent a message or performed an action that is logged in a secure audit trail.

With the Internet frenzy that currently dominates the popular and business press, security for organizations linking their users to the Internet or putting up their World-Wide Web Page, Internet security has naturally become the central topic of security discussions today. The conventional concern is to prevent intruders from breaking into corporate systems. A whole specialty has arisen to help customers establish firewalls that isolate production systems from intrusion; however, it is at least as important to include intrusion detection as part of the multi-faceted security of our organizations.

Other Internet-related problems include concerns over the security of credit-card information and other electronic commercial transactions. Effective encryption solves most of these difficulties while the data are in transit, but it is essential to protect these data while they are on the servers, where they are most vulnerable to unauthorized access. All confidential client data should be discarded as soon as possible (given the business reasons for storing them at all) and encrypted while they are on company servers.

But a different kind of Internet security problem seems to be less frequently discussed: the risks of having untrained employees accessing the vast pool of information available through Internet connections. Inbound access has its perils, as managers at various organizations have discovered when their employees used corporate systems to obtain and store large numbers of pornographic images — much to the horror of their public relations staff.

Outbound Internet access also has its dangers. Every corporate user who posts a remark in a news group or sends e-mail to a correspondent is indelibly marked by their Internet ID. Regardless of written protestations, anyone with an ID that reads markm@megacorp.com is going to be seen as representing MegaCorp whether they intend to or not. Flaming people, sending out false information, and even participating in certain news groups may get an employee and their employer into trouble. Some years ago, a correspondent of the RISKS FORUM DIGEST reported that certain news groups have been monitored by "snitchbots," programs that automatically send e-mail tattling on employees who post messages catering to criminal hackers and virus writers. Imagine having the e-mail directed to the news media and you see the risks.

Another sort of problem caused by inexperience is illustrated by the story of a poor soul who misguidedly put company advertising in several dozen places on the Internet. He was mail-bombed by angry Internet users and his company's 800 phone number was posted to several news groups in the alt.sex.xxx area as a free phone-sex line. The lines filled up with irate heavy-breathers, normal customers couldn't get through to place orders, and one receptionist resigned in indignation at the suggestions she was receiving from the unwanted callers.

Dial-up lines pose an increasing threat because of the popularity of unauthorized entry among the criminal hacker crowd; token-based authentication is the strongest impediment to their depredations. Certainly a dialup line should be encrypted if at all possible. Another defense is to prevent any identifying information whatsoever to be received by a caller until identification and authentication are complete: no modem model number, no operating system version, no welcome message — nothing.

An even greater threat is unsecured access to phone switches. Phone phreaks are estimated to causes billions of dollars of damage a year in the U.S. and Canada by stealing phone services. To prevent unauthorized callers from racking up massive phone bills for their victims, it should be impossible to obtain access to an outbound phone line by calling into the PBX. Operators should be trained to refuse manual connections of this sort. Anyone needing to bill their phone calls to their employer should be issued a phone card (one *without* the PIN printed on the card); there are limits on the liability such a card confers on the organization.

Viruses continue to be a nuisance; however, the range of effective anti-virus tools has been keeping pace with the worst inventions of the evil crew who waste people's time with their wretched creations. The biggest difficulty is macro viruses, which travel in documents and are now often transferred via e-mail. Until we get more effective heuristic anti-virus tools, we still have to try to teach users to be suspicious of unsolicited, unexpected attachments. No one should run an executable file received from a stranger or even one sent by a friend.

Recently there has been a novel form of replicating information in cyberspace: fraudulent warnings about viruses. The “Good Times” hoax, launched in November 1994 by two students, has repeatedly resurfaced over many years through panicky and unverified warnings sent by novices through the Internet, commercial networks and BBSs. Unfortunately, the availability of strong programming languages at the heart of popular office programs created by Microsoft has led to the real-world equivalent of what was once a mere lark: there are now e-mail messages which truly can cause harm when one reads them.

In summary, these problems can be minimized by careful consideration and implementation of corporate security policies, including policies for official use of the Internet.

But the time to do it is now.