

What's Important for Information Security: A Manager's Guide

By M. E. Kabay, PhD, CISSP

mkabay@compuserve.com

Associate Professor of Information Assurance, Department of Computer Information Systems,
Norwich University, Northfield, VT 05663-1035

Copyright © 2000, 2002 M. E. Kabay. All rights reserved.

1 Introduction: why bother with information security?

The basic reasons we care about information systems security are that some of our information needs to be protected against unauthorized disclosure for legal and competitive reasons; all of the information we store and refer to must be protected against accidental or deliberate modification and must be available in a timely fashion. We must also establish and maintain the authenticity (correct attribution) of documents we create, send and receive. Finally, the if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings; if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems.

Another issue that is emerging in e-commerce is that good security can finally be seen as part of the market development strategy. Consumers have expressed widespread concerns over privacy and the safety of their data; companies with strong security can leverage their investment to increase the pool of willing buyers and to increase their market share. We no longer have to look at security purely as loss avoidance: in today's marketplace good security becomes a competitive advantage that can contribute directly to revenue figures and the bottom line.

Part of my job is to collect and analyze above-ground intelligence: news items from news wire services, publications such as NewsScan, reports in Risks Forum Digest, and so on. My impression from all of this reading is that non-specialists believe that criminal hackers are the most important threat to information systems security. However, everything I know about information security contradicts this belief. This paper is an attempt to dispel some of the misinformation about security circulating among non-specialists and to provide practical guidelines to managers for significant improvements in securing information.

2 Threats to Information Security

It is very difficult to estimate precisely what causes damage to information systems. Managers should be skeptical of any statistics about information security if they show very precise numbers. The problem is twofold: people don't recognize crimes or damage, and when they do they usually don't report them anywhere that collects statistics. Surveys that report on computer crime and other breaches of security are useful, but all of them suffer from the problems of voluntary compliance — the fundamental question of whether people who respond to questionnaires are representative of everyone in the field even though many people refuse to participate in the studies. Despite these problems, information security experts generally agree on some rough guesses about how damage occurs.

2.1 Internal dangers

Perhaps half of all the damage caused to information systems comes from authorized personnel who are either untrained or incompetent. Another quarter or so of the damage seems to come from physical factors such as fire, water, and bad power. Maybe a fifth of the damage comes from dishonest and disgruntled employees. Computer viruses cause another few percent, and maybe about 5 or 10% of the damage is caused by external attack.

2.2 External threats

The growth of Internet connectivity is altering these statistics. Many systems were once restricted to internal access, with maybe a slow modem or two for remote access by employees. Today we see production systems (those on which organizations depend day by day for continued operations) nonetheless being opened to access via TCP/IP connections from the wider Internet. Many organizations are also linking their systems tightly with those of trading partners using virtual private networks (VPNs) that increase the number of people allowed to access the systems.

Who are the people attacking computer systems? There seem to be the two major classes: amateurs and professionals. Amateurs include poorly-supervised children, rebellious and badly-socialized adolescents, and psychologically disturbed or ideologically warped adults.

Some amateurs cloak their destructive badly-protected computer systems in the language of social responsibility; they claim to have the best interests of their victims of heart. Their actions belie their words, however: well-meaning people do not place obscenities and insults on other people's property as these cybervandals do on many a Web site.

Hobbyist attacks have recently become a major problem with the widespread availability of tools for distributed denial-of-service attacks (DDoS). Using these tools, even children can locate vulnerable sites on the Internet, implant special “zombie” software, and then later activate the zombie programs to send streams of spurious requests to one or more selected victims. Under siege from dozens or even hundreds of zombie programs, many such victims are swamped by the volume of traffic and see their response time for real customers and visitors increasing unacceptably.

Professionals are harder to characterize, since there are probably fewer of them and they may be harder to catch; however, some criminal hackers are earning a living with their skills. Some professionals use public and illegal sources of information to help unscrupulous private investigators. Some computer criminals steal credit card numbers and sell them to the criminal underground or participate in theft of services from telephone and mobile-phone companies. An unknown number may be involved in industrial espionage.

The use of Microsoft Office products has greatly increased the vulnerability of users because of Microsoft's decision to include a powerful scripting language at the heart of its word-processing, spreadsheet, presentation, database and e-mail products. E-mail can therefore carry documents that include the equivalent of programs— macro viruses that can not only harm documents but also call system routines and therefore wreak havoc with the operating system, memory and files. Other contributors to trouble include scripting languages used on Web sites (e.g., ActiveX, Java, Javascript) and even the fundamental formatting language of the Web, the HyperText Markup Language (HTML). All of these tools have been misused to harm users.

Some criminal hackers have set up shop as security consultants and offer penetration analysis and consulting services for their clients. There is a serious question about the trustworthiness of people who used to break or skirt the law and now claim that they no longer do so; some security experts argue that leopards have indelible spots, whereas others are willing to believe that there is such a thing as an ex-hacker. I strongly urge managers considering hiring such people to ensure that their contracts include severe penalty clauses if any of their employees are found to be breaching client confidentiality in the course of their duties.

2.3 Attractive targets

Several factors influence the likelihood of attack. For example, a small, obscure tool-and-die company with eight employees is unlikely to be as attractive to any external attacker as a major corporation with thousands of employees and a significant share of its market. It is possible that having a public Web site makes an organization an attractive target for cybervandals. Any site proclaiming its tight security is likely to attract the attention of the amateurs who were trying to prove their prowess; for example, security firms are under constant daily attack. Some amateurs deliberately attack financial institutions and military systems to demonstrate their weakness and ostensibly to force improvements. Finally, some hackers attack sites for political purposes; recent attacks on such victims as Indian nuclear power company Web sites are said to be examples of “hactivism.”

3 Basic Protection: Safe Hex

Many security specialists focus on significant improvement to commercial information systems by encouraging basic protection mechanisms. Experts focus on the most important security processes so that clients spend their resources where there will be the greatest return on their investment. This approach is a simple application of optimization theory, from which we know that in any field, there is likely to be a small number of factors that predominate in determining results; some people refer to the Pareto Principle, claiming that 80% of everything is the result of 20% of the causal factors.

The basic problems security specialists see in the field are inadequate security policies, poor training, inadequate security awareness, bad management, improper use of security technology, inadequate maintenance of security and operating system software, and lack of computer emergency preparedness.

3.1 Policy, Power and Position

Many firms have no security policy at all; others have policies that are so old that no one remembers their details (or sometimes even their location). Policies are an expression of an organization's values; if security is relegated to shelfware, employees will act accordingly. Too often, security is an after-thought; someone is assigned the task of managing security but lacks defined responsibilities, has no authority, and can serve solely as a figurehead. One of the most innovative measures in the industry is the recognition of information systems security as a responsibility equivalent to stewardship of financial resources or of operations. The Chief Information Security Officer (CISO) reports at the same institutional level as the CEO, CFO, and CIO. Making the information security officer report to the head of information technology is a conflict of interest; one would not want the chief auditor to report to the head of financial operations; the same principle of separation of duties should apply to security.

3.2 Training & Awareness

Some organizations make new employees go through training in their first weeks on the job. Unfortunately, fewer organizations bother to continue the process of training. Even if technology were not constantly changing, it would make sense to refresh the memory of employees on critical issues such as security. In addition to formal courses, employees should be stimulated to consider security an intrinsic component of their work. Like quality, security is a process, not an end-point. We know that many intrusions or abuses of secured systems are accomplished by so-called social engineering: employees are too often willing to give away valuable information to strangers in response to a personable voice and friendly tone. It is lack of awareness that allows criminals to take advantage of innocent and overly trusting people. Security awareness programs should involve committed, repeated germane examples in of security violations in organizational newsletters or bulletins, and occasional security drills that can be turned into an enjoyable exercise in perspicacity and intelligent response.

3.3 Hiring, Management & Firing

Although management issues such as hiring and firing are not as exciting as criminal hackers and industrial spies, it remains true that an organization's security is in a hands of its employees. All applicants for positions with responsibilities for or even contact with corporate information systems should have their backgrounds thoroughly verified. Managers should remain sensitive to changes in behavior in their employees; the classic sign of crooked employees is exaggerated fear of being absent from the systems they are diddling. All employees should be required to take their vacations; one wants to see that systems continue functioning normally in the absence of any specific person. When employees, contractors or subcontractors are fired, it is essential that information security staff protect corporate resources against future unauthorized access by these ex-employees.

3.4 System Administration

This is not a place to discuss technical aspects of security in detail. Managers should fulfill their legal and professional obligations by supporting technical staff at least for basic system hygiene: establishing a sound security architecture; staying up to date in the versions of security software and operating systems; monitoring intrusions using widely available auditing and intrusion-detection software; and establishing computer emergency response teams so that the organization can intelligently respond to accidents and attacks. Managers may also want to investigate the growing number of security assessment or evaluation services.

3.5 Establish Effective Security Configuration

Any system with links to the Internet should have a properly-configured firewall to implement security policies governing access to corporate data. A firewall is a device that filters packets to and from the Internet, allowing control over what kinds of commands can be carried out on corporate systems by remote users. Many firewalls are improperly configured; many Internet-visible systems are often undocumented and therefore poorly protected. Another frequent problem in network design is that there are no internal barriers to access; firewalls should be placed strategically within an organization to reduce violations of security policies by employees and to limit the damage that can be caused if the external firewalls are breached.

3.6 Maintain Software

Perhaps the single most important problem we face in managing security is that system personnel fail to keep their software up to date. Every system manager must subscribe to the alert services from their vendors and from the Computer Emergency Response Team Coordination Center (CERT-CC at <http://www.cert.org>) and must implement all security patches as soon as possible. Almost all the intrusions carried out by criminal hackers take advantage of known vulnerabilities; failing to heed the free warnings from CERT-CC and one's own vendors is simply asking for trouble. In my opinion as a non-lawyer, such failure to keep current constitutes negligence.

3.7 Detect Security Breaches

One of the changes in the security paradigm over the last few years has been a realization that we will not succeed in achieving perfect security. Our perimeters will be breached; authorized personnel will make mistakes; there will occasionally be problems stemming from dishonesty or from revenge. It is therefore appropriate for us to detect such breaches and be prepared to respond intelligently to them.

The least responsive approach to detecting problems is to examine log files or audit trails. The disadvantage of this approach is that one detects problems long after they have occurred. A better tool — one that complements a good audit trail — is a modern intrusion-detection system. These software tools identify unusual patterns of system use. Depending on their sensitivity, they can flag anomalous behavior by internal personnel (e.g., having an accountant login to the financial system at three in the morning) as well as spotting intruders by recognizing attack profiles. Such software can be programmed to alert system management to a potential problem using a variety of tools; e.g., alarms, e-mail, pagers and even telephone calls.

3.8 Respond Intelligently

There is no point in detecting a problem if we don't have a response in hand. A computer emergency response team (an internal CERT — distinct from the CERT-CC) should be in place before there is a direct need for it; an emergency is hardly the time during which to define and refine procedures. The CERT should include legal staff with expertise event damaging the evidence that law enforcement will require for effective prosecution of the malefactors. Emergency response involves more than a technical battering down of the electronic hatches; organizations should prepare for liaison with law enforcement authorities and have a well-organized public relations plan to keep employees, stockholders, and the public accurately informed of events when conditions allow such disclosure. Some organizations include mechanisms for entrapping external attackers in simulated areas with supposedly sensitive information; these so-called honeypots give the CERT and law enforcement experts more time to locate the intruders and plan for their arrest. All of these plans have to be sought through and tested many times for they are used. Ideally, the CERT will be part of the corporate disaster recovery team because so much of their work will overlap. However, many aspects of the CERT plans must remain secret to maintain effectiveness against internal attackers.

3.9 Use Independent Security Evaluations

Many organizations recognize the benefits of using formal guidelines and methodologies from neutral third parties in establishing their security policies. Some groups have never developed policies; others have been unable to devote enough time to maintaining those policies. Sometimes the information technology staff lack expertise in information security; other times upper management have refused to support the measures known by the staff to be important for protecting corporate information assets. In all these cases, external organizations such as consultants, professional associations and certifying authorities can serve a useful purpose to alter the corporate culture and make the best use of security expertise.

4 Concluding Comments

In summary, managers must understand that security cannot come by buying and installing a gadget, no matter how good. Security is a process, much like quality assurance. Security can and must be woven into the corporate culture of every organization, with due attention to the changing landscape of market advantage, threats, vulnerabilities, risks of damage and extent of damage.

5 For further reading

Look through the other articles on my Web site at <http://www2.norwich.edu/mkabay/index.htm> and in particular “Information Security Resources for Professional Development” at http://www2.norwich.edu/mkabay/overviews/infosec_ed.htm and http://www2.norwich.edu/mkabay/overviews/infosec_ed.pdf

Check out the INFOSEC Newsletters archived on the NetworkWorld Fusion Web site at <http://www.nwfusion.com/newsletters/sec/>

For a single-volume compendium of information security principles and practice, see

Bosworth, S. & M. E. Kabay (2002), eds. *Computer Security Handbook, 4th Edition*. Wiley (New York). ISBN 0-471-41258-9. 1200 pp. Index.