Securing your business in the age of the Internet

by M. E. Kabay, PhD, CISSP
Security Leader, INFOSEC Group, AtomicTangerine, Inc.

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

Information technology is permeating all aspects of modern life and business. The growth of the Internet and in particular of the World Wide Web presents increasing challenges to information technology and business managers.

Coping with Changing Risks

Whereas networks were once primarily internal, many are now exposed to the Internet. Managers must cope with risks on a daily basis and many firms lack the resources to allocate their efforts wisely. Traditionally, information security has used a fortress mentality: managers and technical staff have acted as if perfect security were attainable. However, because of the increasing access to networks due to Internet connectivity, threats and vulnerabilities have grown explosively. Today, security must be regarded as a process, not a stable state. We have to focus on the most significant risks; theory provides a multitude of possibilities, but real-world experience tells us where to put our efforts most constructively.

Clients often ask how security analysts evaluate customer security. We start with an understanding of the fundamentals of information security: protection of the client's confidentiality, control, integrity, authenticity, availability, and utility of information. These aspects of information security uniquely and completely define what our clients need to protect. However, specific threats and vulnerabilities lead to risks that often involve several of the fundamental imperatives of security. In addition, criminals often do several kinds of damage during their intrusions; for example, criminal hackers may not only deface a Web site but also implant unauthorised code allowing for future unauthorised access to the compromised system. Finally, there are many threats and vulnerabilities that are theoretical or potential rather than realistic or actual. Therefore, security analysts have developed a heuristic framework for discussing the most critical aspects of a customer's information systems architecture and implementation in those areas that are, in our experience, most important and most susceptible to improvement at reasonable cost.

We look at security from a number of viewpoints during the evaluation phase. At each step we consider threats, vulnerabilities, consequences of breaches, and appropriate countermeasures. The five major areas of examination are as follows:

- Electronic threats and vulnerabilities: sniffing, spoofing, hacking
- Downtime: reduced availability of timely information
- Physical security: controls on access, disaster prevention

- Malicious code: viruses, worms, Trojan horses, nasty applets and controls, bad software
- Privacy: employee, corporate, customer, national security concerns.

Dynamic and Appropriate Policies

Security resembles quality assurance in that achievement of higher levels requires integration of principles into the corporate culture. One can no more add on security as an afterthought than one can add on quality; everyone has to include quality and security in every aspect of their job. Dynamic and appropriate policies involving representatives of the entire organisation are essentials for effective security. A sensible approach is to use existing templates and to adapt the details to specific requirements. As policies are developed and evolve, they must be disseminated throughout the work force, from management to clerks. Ongoing security awareness programs and periodic re-evaluation and adjustments of policies should be planned, budgeted and implemented.

Even the most expensive computer security hardware and software will be useless if employees cannot or will not use them properly. Security depends on adequate training, motivation, and monitoring. Violations of security policies should be treated seriously, but it is equally important to reward compliance.

Human Resources are Key

How does one acquire and retain honest and competent staff? Security specialists should work closely with human resources and the legal department to ensure adequate background checks on all job candidates. A particularly helpful step is to arrange interviews of candidates by their future. Supervisors must keep in mind the importance of noting any change in mood or behaviour of their employees and to respond in a supportive, professional, and non-intrusive way. When employment terminates, security considerations dictate a firm and even-handed response for all employees. Managers should also pay attention to contract staff, being sure to terminate network access codes as soon as contractors or subcontractors leave a project. These precautions are especially important in the run-up to the year 2000 because of the large numbers of external staff currently hired to solve the millennium bug. Finally, once you have a good staff, keep them well trained. Continuous education benefits everyone.

Known Vulnerabilities

Perhaps the single most important principle we have found in the security industry is that known vulnerabilities account for most of the security breaches we all face. In landmark vulnerability analyses by the United States Department of Defense, 66% of 38,000 unclassified computers and networks were easily penetrated using well-known, frequently ancient vulnerabilities that should have been patched years before. For this reason, systematic approaches to strengthening security all insist on keeping technical staff up to date on known vulnerabilities.

Policies Must Not Be Shelfware

Security policies naturally cover many different aspects of operations. Physical security requires adequate safeguards to prevent intrusion into restricted areas. Effective technology such as ICSA-certified biometric authentication involving fingerprints, irises, retinas, faces, and voice- or signature-pattern recognition can materially improve controls over access--and can equally well be applied to controlling logical access to systems. Smart cards and other tokens are also useful tools for identification and authentication (I & A). However, continuing to rely on passwords for high-security applications is unwise. All of our experience in security indicates that people are bad at picking passwords and that too many people don't understand the importance of keeping passwords secret (hence the custom of checking for sticky notes attached to terminals, under keyboards, and so on when auditors evaluate the effectiveness of security awareness training).

Setting the parameters properly on operating systems, firewalls, intrusion-detection systems, and system logging is essential for security. Security specialists often find that many customers entering the security analysis process have used default settings instead of choosing parameters that reflect their security policies. Firewalls help reduce the likelihood of penetration; intrusion detection reduces the lag between penetration and response. Logging enables forensics destination and possible prosecution. All of these elements are valuable in today's environment.

A critical element of security, especially for portable computers, is encryption. With the easy availability of strong, unobtrusive encryption software today, there is no excuse for having sensitive data stored in the clear--that is to say, without encryption. Laptop and other computer thefts are growing from year to year; frequently, the value of the stolen data exceeds that of the hardware.

An area that is often overlooked in security architectures is e-mail. Users can often evade restrictions on inbound and outbound communications imposed by firewalls simply by using e-mail. E-mail should always be the property of the organisation, not of individual employees; this policy should be announced every time an employee initialises the e-mail program. This precaution allows investigation of possible malfeasance and ensures that employees do not develop a false expectation of privacy for corporate e-mail.

A similar approach should govern access to the Web. Using corporate resources for Web access must clearly allow monitoring or logging to prevent the too-frequent abuse of time and bandwidth. In addition, access to pornographic or hateful materials on the Web makes an employer liable for accusations of tolerating a hostile work environment or other employees. Corporate policy should also preclude multi-user games that can bring a network to its knees during peak network periods. A reasonable compromise is to allow such games after business hours.

With those organisations creating their own software, software quality assurance is, as always, an important element in security. Not only should we avoid bugs that cause errors and down time; in addition, we should avoid deliberately-implanted malicious code. Programmers have been known to insert logic bombs which will work to divert resources using some money techniques; effective testing and documentation--especially test coverage monitors that ensure parts of executable code are tested during quality assurance work--can discourage malefactors and catch harmful instructions before they are executed in production. Similarly, it is important to fight external, self-reproducing malicious code such as viruses (e.g., the Melissa macro-virus), Trojan horses (e.g., the BackOrifice program), and worms (e.g., the recent Worm.ExploreZip program). Every workstation and server should be running up-to-date anti-virus software and allowing it to run constantly in background. Every copy of MS-Word and MS-Excel should disable auto-execution of macros. Wherever possible, Word documents to be shared with others should be saved in RTF files instead of as DOC files (RTF files don't include macros). Users should know that unsolicited or unexpected DOC or XLS files, executables or WinZIP compressed files sent as attachments to e-mail should be examined before being opened or run. To prevent automatic execution of Trojans that look like some other type of file, Windows users should disable the action, "Hide MS DOS file extensions where file types are registered."

Viewer programs such as QuickView and KeyView can prevent attack by Word- or Excel-macro viruses.

As ever, organisations must take adequate backups, safeguard them during storage, and destroy data before discarding backup media. Even non-backup electronic media warrant attention. Some word processors leave deleted text in place in files; examination of such files can reveal previous versions of a document, sometimes with embarrassing results. Diskettes and other removable disks are notorious for containing erased information that is perfectly readable using simple tools. Even formatting a disk may not suffice to obliterate all traces of previous data; however, military-grade zeroing programs can write seven passes of randomised data over the entire surface of a disk or in clusters of specific erased files.

Secure Your Web Transactions

Most organisations active on the Web understand the importance of security for their customers and trading partners. Even though the likelihood that any given packet will be intercepted while in transit on the Internet is very low, the business climate today practically demands encrypted traffic for any confidential information going over the Net. Secure Sockets Layer (SSL), for example, is a straightforward tool for satisfying the public demand for secure transactions. It is therefore unfortunate that so many users do not disable caching of SSL pages on their workstations; cached pages with secure information are vulnerable to examination by unauthorised personnel while they reside on disk.

Customer data captured during secure transactions should be safeguarded. Unauthorised release of such data could be a public relations and legal quagmire. In some cases, such

as medical records, unauthorised disclosure may be a felony, depending on the jurisdiction. Customer data should be kept only if they will be used again; for example, keeping a customer's credit card number on file without their explicit instructions or permission is a foolhardy error. Those data that must be kept should be encrypted so that unauthorised employees cannot access information they have no business seeing.

Another critical element of success in today's Internet is a strict privacy policy. Generally speaking, it is a bad idea to try to make money by selling customer data; the public repeatedly expresses its repugnance at having private information revealed to third parties, especially for gain. Whatever you decide to do with customer data, your policy should be displayed clearly and correctly on your Web site.

Problems are CERTain

No matter how good your security, at some point some security measure will fail. Knowing that helps you plan for security in depth, so that a single point of failure does not necessarily result in catastrophe. Furthermore, instead of trying to invent a response when every second counts, it makes sense to have a Computer Emergency Response Team (CERT) in place, trained, and ready to act. The CERT should include members from every sector of the organisation; key members include operations, facilities, legal staff, public relations, information technology, and at least one respected and experienced manager with a direct line to top management. The CERT should establish good relations with law-enforcement officials and should be prepared to gather forensic evidence. The organisation should have a policy in place on how to decide whether to prosecute malefactors if they can be identified. The CERT should be prepared to respond not only to external attacks but also to criminal activities by insiders. Proper logging at the operating system level and from intrusion-detection systems can be useful to the CERT. The CERT plays an important role in disaster prevention, mitigation, and recovery planning.

Use External Validation

It is a truism in quality assurance that no one can effectively test their own creation. The same principle applies to security. It is difficult to see the vulnerability in our own defensive plans. External testing of security can be a cost-effective measure that complements internal and external audits. The difference between an audit and the test is that the former focuses on policy whereas the latter looks at results.

AtomicTangerine INFOSEC specialists use systematic benchmarks developed over many years by famed security pioneer Donn Parker and his colleagues at SRI, Inc. TruSecure from ICSA.net includes several independent evaluations of security; ICSA checks compliance with TruSecure requirements reported by the customer and then ICSA analysts challenge Internet-visible systems using a wide range of the vulnerability-assessment tools. Many of their clients need more than one pass to achieve TruSecure certification. In Britain, one of the options available to an organisation for testing its

information security is C:CURE, a test procedure based on BS7799. Many consultancies offer systematic evaluation of information security preparedness.

When choosing external vulnerability analysts, companies should look carefully at the backgrounds of the employees who will be checking security. I do not recommend employing firms having active or recently active criminal hackers on staff.

Concluding Remarks

In summary, managers must recognise that security requirements change all the time. Keeping up-to-date is not a luxury, it's a necessity. Getting buy-in from every part of the organisation is a key to success in security as it is in quality. Ensuring that employees are chosen with an eye to honesty and reliability, and then managing employees carefully to prevent dissatisfaction and to identify those at risk of becoming dishonest are crucial to securing information and other corporate assets. Appropriate tools for securing systems and networks include anti-virus products, firewalls, intrusion-detection systems, e-mail logging, and proper backups. A CERT makes sense to prevent panic and disorganisation when problems inevitably occur. External testing of security makes sense for most organisations.