THE INTERNET SHOULD BE A BOON TO YOUR BUSINESS. Your customers and competitors are all there. It provides cheap, 24-hour global access, and makes it easy to link up with your partners and prospects.

But most users believe the Internet is unsafe and fear it for this reason. This lack of confidence is one of the greatest obstacles slowing the profitability of most Internet commerce. If you do business on the Internet, you are obliged to make sure your assets are adequately protected. If you participate as a user or a customer you should know what the risks are and how to manage them.

Opening your business to the Internet exposes it to a vast number of unseen potential attackers. Attackers are more numerous than ever and several trends favor them:

- The Internet has grown far ahead of the technical people and tools available to protect its users
- Much of the technology is new and immature, with the unpredictability that entails
- The business processes are new, too, without the safeguards of fully developed practices

The problem is not software. The problem is people. With few exceptions, hackers exploit human errors, not core technical vulnerabilities.

You may be charged with convincing your company's management that risk to company assets is properly mitigated. The way to do that is by creating and implementing a security policy.

When data is sent from one computer to another on the Internet it makes dozens of "hops" from one intermediate machine to another. Every
computer inbetween presents an opportunity for prying eyes to see what is being sent. This poses an obvious security problem. There are several solutions:

Prevention — Keep problems from occurring in the first place.
Vigilance — Keep on top of events at your site; don’t assume that “all quiet” means you are safe.
Remediation — When problems come up, fix them immediately.

**STEPS TO MAKING YOUR SITE SAFE**

- Know what your assets are
- Know what your risks are and how to mitigate each one
- Educate your users
- Lock down the superuser/administrative user IDs
- Make sure your system is physically secure
- Take “trust” out of your organization
- Create a comprehensive security plan
- Hire, train, and manage the best system administrator you can find
- Minimize your system’s exposure to the Internet
- Find and fix all known security holes
- Stay current on news about new ones
- Create an ongoing defense plan
- As you do more on the Internet, expand your security work to keep pace

**Computer Security Basics**

A computer system is called “secure” when the following conditions are established:

- Integrity
- Access control
- Authentication
- Availability
- Confidentiality
- Nonrepudiation

There are two sources of vulnerability:

- Outsiders — Barbarians at the Gate: “If you build it, they will come”
- Insiders — The Enemy within the Walls

Your site may be used as a base for attacks on other sites.

Some hackers are criminals. Most are a mere nuisance, like vandals. Given the choice between the thief who steals your car and the vandal who scratches the paint, most car owners will choose to avoid them both. This chapter explains how to do that without keeping your wheels locked in the
garage. It is for nontechnical people who need a practical approach to computer security.

DEFINITIONS

This chapter uses the term “hacker” to mean anyone who tries to get in where you, the system owner, do not want him or her to go. The following characteristics are not relevant:

• **Motivation.** It does not matter whether the hacker has illegal or malicious intentions, or is just curious
• **Success.** An attempt at illicit entry is not innocent just because it is unsuccessful
• **Stranger or insider.** Anyone who goes where he or she is not welcome

In computer industry terms, a “hacker” is anyone who delves into the inner workings of computer hardware or software, and a “cracker” is someone who uses this arcane knowledge in a malicious way. For the purpose of this chapter, a hacker is anyone who wants to get in where you do not want him or her to go.

GOALS FOR INTERNET SECURITY

No Internet site is perfectly safe. The best approach for a business-oriented Internet site owner is the following:

• Assess and understand what your risks are
• Take a series of measured preventive steps to comprehensively manage this risk
• Make site security an ongoing part of your organization’s daily work

Since “perfect safety” is not the goal, what is? The goals in securing your site is to:

• Raise the cost to potential attackers
• Make sure site manager can detect a violation and react to it quickly
• Contain and minimize potential damage
• Make recovery as easy as possible
• Install strong security measures that enable you to present your site as “certified secure;” use this as a selling point privately with your customers; do not advertise it too loudly

COMPUTER SECURITY FUNDAMENTALS

• Sooner or later someone will attack your site
• An attack is defined as any attempt to get access to more system resources than the system owner intends the user to have
• An unsuccessful attack is still an attack, and the attacker should be identified and held accountable for it
• Your system has hundreds of features you don’t know about, and will probably never care about. Many of these features make it vulnerable to attack
• Most operating systems are insecure in their default configurations; they come out of the box with widely known default passwords and most of their security features turned off
• Find out what the security features of your system are; turn them all on
• Get all available patches for your operating system and applications, and install them; many of these patches close security holes, whether published or not

Tips
• Most logging facilities are turned off by default. Turn them back on. Historically, logging was turned off because it consumes lots of disk space. In the late 1990s disk space became cheap, and dropping by 50 percent per year, so you can afford it.
• Backup your files thoroughly and often. It is an excellent low-cost way to limit the damage from a virus or malicious attacker.
• Do not store credit card numbers on any machine that is connected to the Internet. That goes for any other data that absolutely must not be accessed by unauthorized users.
• Most e-mail traffic is extremely insecure. Do not put anything in an e-mail message you would not want to be made public. If your e-mail must be kept confidential, use e-mail encryption.
• Limit the questions your staff put on Usenet, especially with regard to security and system configuration.

RISK
What are your risks?
• Your firm’s reputation, and the trust and confidence of your customers.
• Destruction of data and equipment crucial to the operation of your business.
• Loss of the investment in time spent on your Website.
• Expense of the cleanup.
• Loss of business due to your site’s downtime.

Assessing risk
If your data are extremely sensitive, such that theft, loss, or tampering would cause loss of life or imperil the future of the company, it should not be on any machine that is directly or indirectly connected to the Internet. Store it on a machine that is accessible from your internal network only.
Identify your assets. Inventory all hardware components and software including third-party products, utilities, home-grown applications, driver programs, and operating systems. Identify all data — online, archives, backups, and even users.

If your Website is a “brochure” site, with static pages of sales material, consider the cost of developing it and the expected sales benefits that would be lost if it were tampered with.

Assume there will always be holes and vulnerabilities you do not know about. This is all the more reason to close every single hole that is documented. No hole is too small.

In the 1970s, security holes were allowed to remain open in the belief that they were accessible only to a tiny number of “experts.” Today, the information is easy to find, and well-engineered “burglar’s tools” obviate the need for a high level of technical talent.

Cost-Effective Risk Management

- Limit the assets you expose to the Internet
- According to CERT (see References), the majority of breaches come from weak passwords. Weak passwords are 100 percent preventable (see Password Guidelines)

Types of Attack

Typical attackers’ objectives include:

- Deleting files from your site
- Changing passwords so authorized users cannot log in
- Stealing online assets, such as competitive information
- Stealing files that can be used for commercial gain, such as credit card numbers

Hackers search for one weak point or pinhole in your site’s security. Attacks are typically carried out by making a small, crucial changes to your system. For example, some remote login utilities may be secure in themselves, but are a little too verbose in that they tell outsiders what operating system and version you are using. Once a hacker knows that, he can research the security bugs in that OS, and he is off and running.

A good example is the German hacker detected and finally caught by Cliff Stoll in *The Cuckoo’s Egg*. The hacker exploited an obscure bug in an e-mail program that allowed him to substitute his own version of a system executable file on the victim’s system. This one change allowed him to make several other changes, each one small, and eventually run rampant through the victim’s system. Stoll first detected the miscreant only by careful reading of system audit logs. He tracked the hacker’s activity across
many other systems. Virtually all of the other system managers were un-
aware of the hacker. Some of the systems were owned by the U.S. Depart-
ment of Defense and thought to be impregnable. The hacker was
competent and persistent, but no guru. Yet he was enormously successful
in breaking into dozens of systems, and took part in a worldwide scheme
to steal U.S. government secrets and sell them to the (then) Soviet Union.
The e-mail bug that gave him a foothold was widely known and quickly
fixed by the program’s author.

Intrusion consists of either an unknown person gaining access to your
system’s resources or a known person accessing resources not intended
for him or her. Results of intrusion are modification and/or loss of data,
breach of confidentiality, denial and/or disruption of service.

Note that many intrusions are carried out for the purpose of making
your system the base for attacks on other systems.

THE SYSTEM ADMINISTRATOR: CARE AND FEEDING

To protect your site, you must manage, train, and motivate your system
administrator (sysad). The sysad is charged with keeping hostile elements
from damaging your system. The sysad’s job objectives are

- Establish confidence in the integrity of the system
- Minimize risk to the company’s system assets

The above objectives are accomplished by planning, designing, and im-
plementing technical measures and organizational programs within the en-
terprise. If this sounds more demanding than setting up PCs and backing
up files, it is.

- Invest in training to keep your sysad’s skills up to date
- If your sysad does not have time to pay adequate attention to security
  issues, restructure his or her duties
- Establish a career path for system administrators; after 2 or 3 years a
good sysad should be kicked upstairs; this works wonders as a moti-
vational and recruiting tool

There will always be new bugs and holes to take advantage of. Despite
this, the hacker’s best path into your system is by social engineering. This
means getting to know the sysad, calling up posing as a user with a forgot-
ten password, and watching the Usenet newsgroups for questions or prob-
lems that indicate vulnerabilities. An attacker may be able to get into your
system, despite all its safeguards, by finding a “helpful” employee who
gives away more than he or she should.

Vendors’ notification of security fixes is usually limited. Announcements
typically go to security-related newsgroups and mailing lists only. It is the
sysad’s job to monitor these actively and keep the system current.
Recruiting Your System Administrator

Hire the best sysad you can find. Get one with real experience in security, not only in system management.

When interviewing candidates, ask the following:

• If his or her previous sites have had explicit incident response procedures
• If he or she has handled a break-in, or break-in attempt, or other incident of unauthorized resource access, malicious or not
• Which system services are typically turned off for Web servers

Here is a list of preventive measures from Farmer and Venema (see Notes). Your sysad candidate should be familiar with them:

• The finger service can reveal things about your system’s OS and users that no one needs to know; disable it or replace the program it with a less “generous” version
• Export read-write file systems only to specific, trusted clients
• Alternatively, export read-only file systems only
• Restrict the ftp service, and disable tftp
• Disable NIS
• Get a list of machines that have “trust” relationships (see Definitions) with your own machines; a “trust” relationship means the machines mutually allow cross-logins without password verification; this means that the security of your machine is out of your control, never a good thing
• Consider eliminating trust entirely

The sysad weekly status reports should include the following:

• Any relevant security advisories received and implemented. There are typically several new CERT advisories (see References) every month
• System monitoring and auditing work done
• Maintenance work done to keep the site secure
• Software patches made available by vendors
• Software patches applied
• All user accounts added, deleted, or modified, with all privileges listed

Design your site to play to your sysad’s strengths. If your staff does not have UNIX experience, get a Microsoft Windows NT box.

Ironically, hackers see the sysad as their primary pathway into the system. A common tactic is for a hacker to target a site after he makes a study of the sysad’s habits, skills, and weaknesses. Your sysad must be mature and capable enough not to be vulnerable to these tactics.

MANAGEMENT STRATEGIES

If you engage an ISP, you are dependent on them for security. As a rule of thumb, the more things you run on your machine, the more security
holes there likely will be, so your Internet server should run only the re-
quired minimum of services. Ask your Internet Service Provider if the same 
machine on which your data resides is running mail, POP3, NNTP, print 
serving, FTP, or login authentication. With each extra service, the likeli-
hood of a security hole greatly increases.

SYSTEM AUDITING

A system audit lists all accounts and their privileges for every server 
and workstation, and all trust relationships.

In general, you should adopt several overlapping strategies and combine them at low cost.

1. Explicitly deny all services, file access, etc. except those specifically allowed
2. Restrict, monitor, and audit access

Establish your enterprise’s acceptable risk level. If you can’t tolerate any risk, you shouldn’t be on the Internet at all.

Connect only the required minimum of your network to the Internet, and assume it will come under attack by hackers. Put everything else behind the firewall.

SOURCES OF INTERNET MALFEASANCE

Your system is at much greater risk from your own employees than from hackers or computer criminals. Data security professionals at large compa-
ies typically spend 90 percent of their time making sure the internal staff are able to see and do only what their duties entail, and nothing else, and that they handle this responsibility professionally. They spend only small fraction of their time worrying about intruders, and so should you. In al-
mmost all cases, more valuable information walks out on floppy disks then will ever be taken by hackers.

Internal breaches are made by company staff who are supposed to have some access to the system, but contrive to get more. They may want to look in personnel files, pirate software, read the boss’s mail, or just grab some extra disk space. Many fall into the “disgruntled employee” category.

An insider can see passwords taped to the front of terminals. Most compa-
ny staff place assets at risk through carelessness and ignorance. As a manager, your time and budget will be very well spent working on these.

Internal staff who try to break into system resources they should not use have a variety of motivations: mischief, ego, boredom, or personal con-
licts with other staff members. Some will say, “I have to break through sys-
tem security to do my job.” If this is true, then your business process is
broken, not your Website. Fix the process and close the hole your staffer used to hack it.

All of these indicate that the business process and your security policy are defective. Fixing these will do much more for your business than worrying about hackers.

More than 50 percent of vulnerabilities come from sheer carelessness. To test your own site’s security, try this social engineering test: pretend to be a sales rep, and phone in from the field with an emergency system access problem. Tell the system administrator you just need a favor to get out of a jam — having a password reset to a known value, or access to a dial-in number.

Next, pretend to be a system administrator. Phone a field sales rep and say you need his or her password to “fix a system problem.” If either of these scams succeed, you have a problem.

The bane of the system administrator’s existence is the employee who asks for a favor in violation of the Security Policy and says the sysad had better accede to his or her request or the boss will get ticked off. If you are the boss, make it clear ahead of time that you will support the sysad in refusing requests of this kind.

In large organizations, a basic assumption is that most internal theft will occur in small amounts over long periods of time. For this reason, an employee who is found misappropriating even a tiny amount is immediately subject to firing and prosecution.

**HACKERS**

Most hackers are like vandals — a costly and damaging social nuisance; only a minority are in it for profit.

The most dangerous person is not the unknown outside attacker but the malicious insider with sanctioned business on your system. Much more valuable information leaves victims’ sites by floppy disk and voice phone calls than by outside intruders.

A common tactic among hackers is to watch newsgroup messages and bulletin boards for messages signed, for example, “Richard Roe, System Administrator, XYZ Corporation.” Let’s say the newsgroup is devoted to baseball, and Mr. Roe says he is a Boston Red Sox fan. The hacker goes to the site and attempts to break in with passwords like “RedSox,” “pennant,” and so on.

A related tactic is to send Richard Roe e-mail, claiming to be another Red Sox fan, and begin a long exchange of e-mail messages. In the course of online dialogue, the hacker learns Mr. Roe admires former Red Sox star
Ted Williams. He goes to the site, tries “TedWilliams” or “400hitter” and bingo! Without using any technical skill the hacker comes in through the front door.

Never put anything important in an e-mail message. This especially applies to passwords and credit card numbers. The first thing most miscreants do is scan the mail directory for the words “password” and “Visa.”

The scheme should be fail safe. If the system fails it should fail harmlessly. Just as the way a car’s steering wheel lock makes the car more difficult to steal, the best approach is to deter hackers and make them move on to easier targets.

When Protection Is Not Protection

Several security schemes purport to protect your data, but in fact provide little or no protection. These may keep the honest people honest, but do not rely on them to provide any real security.

Security by Obscurity. Hackers’ tools exist that will scan an entire site and show its complete directory structure. It will not work to put valuable files in an out-of-the-way directory and assume no one would bother to look there.

MS-Office and Zip File Password Protection. The encryption algorithms for both are known to be weak, and methods of defeating them have been widely circulated. If you must encrypt a file, use real encryption software such as PGP and F-Control.

SECURITY POLICY (INTERNAL)

There are two approaches to this, a “zero-based” approach and an “everything but” approach.

- Zero-based policy: the minimal, additive approach. Each user gets only what his or her day’s work requires. Each system service is enabled with only the minimum required functionality. Explicitly deny all services not absolutely required and justified. The firewall stops everything except those few permitted services, such as e-mail.
- Everything-but policy: the services known to be vulnerable or dangerous are turned off, but most other services are left on. System security manages, monitors, and audits access more than restricting it.

To implement:

- Determine the resources needed for each business process and for each person involved in it.
- Based on this, decide which files and programs to make available
- Lock down all other system facilities
Consider removing the restricted resources from the network entirely. The key is not to take a reactive stance or wait for a problem to develop and try to play catch-up.

User Education

Make sure each user is clear on the following:

- Each person is responsible for his or her own password and anything that is done while using it.
- Each person is responsible for the equipment, software, and login account resources entrusted to him or her.
- Each person is obligated to report untoward system behavior that may indicate an attack.

Computer misuse is just like any other type of crime, and the consequences are the same. Plug the holes in the dike. This approach entails creating a list of known security weaknesses, and takes steps to close each one.

Clearly, your site should use both approaches. You should take the zero-based approach first. Then start the “plug the holes” stage, which will be much smaller and simpler because of the first steps. Most sites start and finish with a “plug the holes” approach, or do nothing at all.

The job of the system administrator and the manager responsible for security is to find creative ways to reduce privileges to a minimum without creating undue complexity, hurting productivity, and making the users unhappy.

Finally, you should reassess your security policy at regular intervals, and whenever a major change occurs.

Incident Response Procedures

Formulate a series of steps to be taken:

- When a breach is discovered in progress.
- When evidence of a past violation is discovered.
- When a virus is suspected or positively determined to be present.

Example: all security warnings/failure reports will be recorded and investigated, with their causes and actions taken forwarded to management. It is the employee’s responsibility to:

- Report possible security breaches.
- Know protocol for handling attacks.

The CERT site is a gold mine of information on this topic. Go to http://www.cert.org/nav/securityimprovement.html.
System Configuration Standards

Keep in mind that most of the areas in which your system is vulnerable are caused by incorrect configuration settings.

Pay special attention to home-grown software. It is rarely built with security in mind. Connect only a limited segment of your network to the Internet. Expect that these machines will come under attack and that some attacks will succeed.

Consider making the file systems on the exposed machines read-only, thus by definition resistant to tampering.

SECURITY POLICY (EXTERNAL)

Your primary external defense is your firewall. A firewall is a group of system components whose job it is to enforce your system’s security policy. Firewalls allow in some traffic and restrict everything else. The critical issue is that you must know what you want your firewall to do, what to allow, what to restrict. This is your security policy. Some firewalls are built using software alone, some use separate hardware components.

To keep out hackers, you need a comprehensive security program. The security policy should explicitly state rules for accessing the system via all available means. If there are dial-in modems attached, specify who is allowed to get in and what they may do. Management decides what will be visible from the Internet. Only those resources are made available and everything else is locked down.

Creating an Internet site means you want your system to be partially accessible to authorized users. “Partially” means that users get to the level of access you specify. If you have a static brochure site, readers may read some of your files, but only the ones you authorize, and they may not modify or destroy them. If your site is interactive, users can enter data where permitted, but cannot wreck or steal the resources the site presents.

PASSWORD GUIDELINES

CERT estimates that 80 percent of problems result from weak passwords. Educate staff on their obligation to maintain secure and unguessable passwords, and ensure they comply. Your site will become much more secure overnight. A “guessable” password is

- Anything you can find in a dictionary — a word, name, place name, abbreviation, etc.
- The company name and the person’s own name are used so often that intruders routinely guess them and frequently succeed.

Hackers often attempt to break into users’ accounts by guessing passwords. This approach is very simple and staggeringly successful.
Common passwords are used so much that this approach is often successful. According to a popular anecdote within the computer security industry, the second most common password is “love.” The most common is a four-letter synonym for “love.” Hint: If your site is dedicated to the study of orchids, the root password should not be “orchids.”

One recommended guideline is that passwords contain a combination of numbers and uppercase and lowercase letters. A popular method is to take a phrase that is easy for the user to remember, such as a movie title, create a mixed-case acronym from it, and use that as a password. For example, “Titanic starring Leonardo Dicaprio and a big boat” would contract to “TsLDa2b2.” This seems like a complex string to type, but it will become automatic within a day or two.

Password rules should be enforced by an automated utility. There are many of these on the market for every operating system. Typical password enforcement functions are

- Require a reasonable minimum password length, usually eight characters
- Automatic password expiration parameters to force password changes quarterly; users generally find monthly password changes to be onerous
- Check for and disallow use of already-used passwords
- Disallow obviously weak passwords, such as the company name, or the user’s name

A widely available hacker’s tool wages a “dictionary attack” which repetitiously attempts automated logins using words in a large dictionary file. If a password is a word in the English dictionary, the program will discover it and so will the hacker.

An especially bad choice is the name of any family member. Working in data security for a large financial services firm, I would routinely see an employee’s desk with a child’s picture and perform the following:

- Ask the name of the child
- With the employee looking on, log in as him and enter the child’s name as the password

This works in an astonishing number of cases. Add the child’s birth date to the name and the success rate climbs even higher. (Stranger still, I could visit the employee again a few weeks later, and log in again with the same unchanged password.)

Use a different password for each system you log in to. If you subscribe to an online Website specializing in orchids, use a different password there from the one that protects your e-mail account or your Website. Many hackers set up sham “promotion” sites, under the pretext of providing free
software or special interest forums, for the purpose of collecting pass-
words.

I met a system administrator who uses the same password for the root
accounts (see Glossary) on dozens of different machines. That password is
an easily guessable word in English. I would like to borrow his ATM card!

PHYSICAL SECURITY

Anyone who can physically touch a machine can break into it. If you
cannot restrict physical access to a machine that houses your system, it is
not safe.

PROFESSIONAL HELP

Penetration-testing companies will attack your site to help your deter-
mine how vulnerable you are. These attacks simulate a real attack.

Consultants from penetration-testing companies provide the following
services:
  • Check your system for technical compliance with security standards
  • Train your staff on how to find and fix holes
  • Provide ongoing strategic and technical advice to keep your site safe

These are consulting companies that field a penetration assessment
team. Their methods are the same as those used by hackers. Their job is to
identify your site's vulnerabilities, and train your IT staff on how to find and
fix them.

Recommendations:
  • Don’t engage a penetration service company that only operates re-
  motely. To do the job they will have to gauge social engineering and
  physical access vulnerabilities. This cannot be done effectively away
  from your site.
  • The assessment team should be knowledgeable about security and
  about your business, not only about technical issues and security
  products.
  • Many companies are concerned about penetration service companies
  learning too much and using the information against them. Select your
  vendor carefully, and talk with the customer references they supply.
  • Costs are typically near the top of high-end IT consultancies.

Keep in mind that the best value is the knowledge retained by your own
staff.
Author’s Bio

Jim Hewitt has worked in data security, system administration, and software engineering for more than 10 years. He has held engineering and management positions in several well-known financial services, manufacturing software and healthcare systems companies in the U.S. and Asia. He is a principal consultant at Brainstorm Technology of Cambridge, MA.

Notes

The U.S. General Accounting Office conducted a test break-in of the U.S. State Department’s automated information system and found it prone to attack. The problems they found are present in many, if not most, companies’ systems.

Most of the best information sources are academic or other noncommercial organizations, and are publicly available. Take advantage of this fact.

To get some insights on how hackers work and think, look into these two usergroups:

Alt.2600
Alt.2600.hackerz

“2600” refers to the frequency of a whistle used by a legendary phone system hacker to fool Ma Bell into providing free phone service.

Other good sources:

- Farmer, D. and Wietse, V., *Improving Your Site by Breaking Into It*, at www.best.com/~mld/unix/papers/improve_by_breakin.html. This is an excellent white paper, focused on UNIX but widely applicable.

GLOSSARY

Trust — A relationship among two or more computers, whereby users who are permitted to access one are automatically permitted on the others.

Firewall — A hardware or software component that restricts outside access to your system.

Service — A function performed by a computer. An example is a print service.

Hole — A defect in a computer program or operating system that allows a breach of security.

Social engineering — Nontechnical break-in methods that use information accidentally divulged by sanctioned system users. Typically this means tricking the victim into revealing a password, or providing clues that allow the hacker to guess it.

Hacker — A technical person who explores the inner workings of computer systems, usually without illegal intentions.
Cracker — A hacker who uses his or her technical skills to illegally break into other systems. “Crack” originally referred to the process of decoding passwords, something like cracking a code.

Root — The “superuser” login account that allows full access to every file and resource on the system, and can create other user accounts. The root password is the keys to the kingdom. Only the systems administration should know the root password.