Framework for Internet Security Planning
Monica J. Garfield
Patrick G. McKeown

Payoff
Internet security is a holistic process that is only as strong as its weakest link. Using an analogy to home design, this article presents a framework for understanding the issues involved in Internet security and assessing available security options.

Introduction
As an easy-to-use interface that supports sound, video, and graphical displays, the World Wide Web is being increasingly employed by organizations of all sizes for electronic marketing and advertising, customer service, and ordering centers. This growing commercial use introduces new opportunities as well as new security risks. Many security concerns stem from flexible design techniques used to build the Internet, some of which make it difficult to identify exactly where data and requests are coming from or where outgoing data will travel.

Hackers are breaking into computers daily to sabotage or explore mission-critical data. Formulating a plan to thwart these curious onlookers and potential computer villains is no easy task, because there are many ways unwanted intruders can attempt to gain access to a corporate computer and a range of measures available to help secure that environment.

Given the loosely controlled Internet infrastructure, the best way an organization can protect its Web environment is to provide security at the front door. Before an organization can do so, Information Systems managers must first ask two questions:

- What is the organization trying to secure?
- What price is the organization willing to pay for this level of security?

The answers to these questions provide the basis on which to formulate a security policy. This paper presents a framework that helps IS managers assess the broad range of issues involved in the creation of an Internet security plan. It does not provide the technical details needed to deploy security measures but rather a road map of the options that should be considered.

Connecting to the World Wide Web
The method an organization chooses to connect to the Web plays a major role in the level of functionality it obtains and the level of risk it faces. Exhibit 1 depicts the most common ways companies gain access to the Web, each of which is associated with different degrees of flexibility, costs, and security risk.

Internet Access Options
### Type of Connection

<table>
<thead>
<tr>
<th>Type of Connection</th>
<th>Enterprise Network Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Direct</td>
<td>Full Direct Connection</td>
</tr>
<tr>
<td>Indirect (through third party)</td>
<td>Full Buffered Connection</td>
</tr>
</tbody>
</table>

**Full Direct Connection**

A full direct connection means that an organization has its own Web server directly connected to the Internet and to its enterprise network. This connection method has the greatest flexibility, the highest security risks, and potentially the highest start-up costs. It gives employees full access to the Web and the enterprise direct control over the Web site.

The actual hardware and software costs to set up a simple Web server are not high—all that is needed is a machine that can run as a server, which can be a Windows-based PC a Macintosh workstation, or a minicomputer, plus server software. This software is typically easy to use and understand. The higher costs associated with a full direct connection result from the organization's need to protect the internal network from intruders. Securing a Web server from potential hackers requires a fairly high level of technical knowledge, because hackers are constantly improving their techniques.

**Full Buffered Connection**

A full buffered connection means that an organization has a Web server connected to the Internet through a third party and directly connected to the enterprise network. This type of connection is comparable to the full connection in terms of security risks but, depending on how the third-party vendor designs the Internet connection, may provide less flexibility. Although the third-party vendor may also set up most of the necessary security components, many companies believe that further security is necessary. Under this configuration, the organization must still purchase and maintain the server hardware and software.

**Standalone Connections**

Standalone direct connections and standalone buffered connections differ from full direct connections and full buffered connections because the Internet connection is not directly tied to the enterprise network. Would-be hackers therefore cannot gain access to the company's network. Likewise, employees may not have a direct Internet connection. This option is the most secure but usually the least flexible.

Many companies are implementing standalone buffered connections, in which Internet access not linked to the enterprise network is provided by a third-party, through
outsourcing. When a company outsources its Web needs, it subcontracts with another company that specializes in creating and maintaining commercial Web pages. The costs associated with this popular option vary significantly. Organizations must weigh the benefit of increased security against the disadvantages of not having direct access to the Internet. Exhibit 2 summarizes the degrees of flexibility, costs, and security risk associated with each of the four connection options.

### Degree of Flexibility, Costs, and Security Risk of Internet Connection Options

| Degree of Flexibility, Costs, and Security Risk of Internet Connection Options |
|-----------------------------|---------------------|---------------------|---------------------|
| Option                      | Flexibility         | Costs               | Security Risk      |
| Full Direct Connection      | High                | High                | High               |
| Full Buffered Connection    | Medium              | Medium              | High               |
| Standalone Direct Connections| Medium             | High                | Low                |
| Standalone Buffered Connections| Medium         | Medium              | Low                |

---

Securing the Network Environment

Securing a corporate network environment is similar to building a house. No amount of amenities can make up for the lack of a well thought-out design plan and a solid foundation. Without these, the house will always be flawed.

Security policies must also begin with a solid foundation in the form of virus protection and password integrity established before an Internet connection is obtained. Once the foundation has been laid, IS and security managers can build strong and secure protection for a corporate network by moving through five levels of security:

- Patching and prevention of security holes.
- Encryption and authentication.
The following sections review these levels and the options available within each.

**Patching and Preventing Security Holes**

If virus protection and password integrity form the foundation of a secure environment, the patching of known security holes marks the beginning of a supporting frame. Many of these holes result from the fact that the Internet, and many of the protocols associated with it, were not designed to provide a high level of security.

One known security hole results from the UNIX operating system, which was designed by computer engineers to make their work easier to manage. The UNIX OS lets an approved user log in from anywhere at any time to administer the system. By gaining access to the root, system administrators can manipulate all files that reside on the UNIX workstation and from there enter a corporate network. Unfortunately, unauthorized users who know how to exploit these features can do the same thing. Fortunately, much of the server software and many of the operating systems can be altered to greatly improve security.

Although a knowledgeable systems administrator can patch many of the holes in the security armor of a company's server or network, others are not so easily fixed and still others are as yet unknown. As a result, one of the best ways to protect mission-critical information is to move it onto other servers or networks that are not connected to the Internet.

Yet some critical information usually needs to be available on the portion of the corporate network accessible to the Internet. Several steps can be taken to improve the security of this information.

**Identifying Security Holes**

One way to begin to detect holes in the corporate server or network is to run a program designed to identify potential security risks. Many of these programs are controversial because they are also used by hackers. Yet it is precisely for this reason that organizations must use the programs, two of which are SATAN (Security Administrator Tool for Analyzing Networks) and Internet Scanner.

Other steps a network administrator may take include turning off unneeded UNIX functions that provide security holes and changing the default passwords. Web servers can also be set up in unprivileged mode, and the root directory should not be accessible. Sending Network File System (network file system) files outside the internal network should be prohibited, and sendmail and mail aliases should be restricted. If file transfer protocol File Transfer Protocol services are necessary, then the network administrator should restrict writable access to FTP's home directory. Files in the anonymous FTP should also not be writable or ownable. Restricting remote log-ins (rlogins) and hiding domain name services also helps secure the corporate environment.
Monitoring Hacker Activity

Once known holes are patched, network administrators need to stay on top of who may be trying to break into their computers and as well as at other Internet sites. Several mailing lists, such those run by the Computer Emergency Response Team Computer Emergency Response Team provide updates of security violations. The alert mailing list, for example, can be subscribed to with an E-mail message to request-alert@iss.net that contains the message subscribe alert. Such information is also available from Web sites.

Because only about 5% of all intrusions are detected and only 5% of these are reported, staying on top of who is trying to break into a corporate computer also requires that server logs be monitored for unusual activities. For instance, one of the new ways for hackers to break into Web sites is to put rogue code onto a Web server by overrunning a software buffer. This gives an intruder unauthorized access to the account under which the hypertext transfer protocol (HTTP) process was running. When oversights such as this are found in the software, the Web server needs to be quickly patched. Copycat hackers are only too ready to exploit the system flaws found and advertised by other hackers.

Encryption Software and Authentication

Once security holes are identified and patched, IS managers should consider encryption software and authentication. Encryption programs let users encrypt their communications so that they cannot be as easily read by unauthorized parties. Using such software can be likened to locking the doors to a house or sealing an envelope. Encryption programs apply cryptographic algorithms to break down ordinary communication messages (i.e., E-mail) into unique codes that can be unlocked only by individuals who possess the unencryption key.

Encryption

Public-Key Encryption.

Public-key encryption is the most popular form of encryption, largely because of the program Pretty Good Privacy (PGP). PGP, which was created by Philip Zimmermann and uses Rivest Shamir-Adleman algorithms to encrypt messages, is freely available on various Internet sites.

The basic premise of public-key encryption is that each user creates two unique keys, one that the user keeps and a public key that the user gives to others. The user then obtains the public keys of the desired recipients of a message and uses them to encrypt a file that only the receivers can unencrypt. Most users also sign their files with a unique signature (i.e., a block of characters) that receivers can verify by applying the sender's public key to the message.

Private-Key Encryption.

Private-key encryption is less popular but considered to be robust. The main advantage of this form of encryption is that it lets users exchange their keys more securely than can public-key techniques. The most popular private-key encryption software is MIT's Kerberos.
Hardware-Embedded Techniques.

Some companies are moving toward encryption techniques embedded in hardware. PCMCIA (Personal Computer Memory Card International Association) cards can be manufactured with the capability to provide secrecy and authentication for the user. This technology is still in its early stages, so its usability and acceptance are uncertain.

Authentication

Various techniques, some of which have no cost and others that are encryption-based, are available to verify the identity of a sender and the authenticity of a message. Authentication becomes increasingly important for ensuring that individuals ordering products over the Web are who they claim to be. Some authentication methods include:

· Stipulating that a sender sign a message by citing something only the receiver and the sender would know (e.g., a discussion the sender and the recipient had the day before, a pet name, a favorite color). Obviously, this method works only when the sender and the receiver know one another.

· Using a three-way hand shake (i.e., sending a first message, having the receiver send a reply, and finally sending the actual communication).

· Using a program that creates a unique digital signature for the user. Many encryption techniques have the capability to create such signatures.

· Embedding a time stamp into an E-mail document. This method is primarily used primarily to verify when a document was mailed for legal suits and contract issues.

Firewalls

Firewalls are the dominant technology used to protect corporate networks from hackers. A firewall is a piece of software that lies between a company's internal network and the Internet and forms a barrier to prevent hackers from gaining access. Drawing from the analogy of home design, the designer needs to decide where to put windows and reinforced doors in the walls of a house. If a company creates a firewall without any windows, people inside the company cannot see out into the Internet and use many of its services. Thus firewall planning involves a tradeoff between user flexibility and the level of security provided for the internal network. Although no firewall is perfect in this attempt, many come close.

Once a corporation decides to put in a firewall, security personnel need to program the firewall to support the organization's security needs. A firewall can be restrictive or flexible depending on the company's goals. For instance, specific services, such as File Transfer Protocol, which is one of the most common ways for a hacker to break into a server, can be limited to reduce the probability of break-ins.

The primary purpose of a firewall is to look at every piece of information that is sent either into or out of the internal network. Firewalls act on a message on the basis of user identification, point of origin, file, or other codes or actions. There are four basic actions a firewall can take when it looks at a piece of information:

· The packet of information can be dropped entirely.
An alert can be issued to the network administrator.

A message can be returned to the sender after a failed attempt to send the packet through.

The action can just be logged.

Several different types of firewalls protect the internal network at different network layers. The two most common types of firewalls are router-based Internet Protocol (IP) level firewalls and host-based application-level firewalls.

**Router-Based IP-Level Firewalls**

The router-based firewall focuses on packets—the basic unit of communications within the Transmission Control Protocol/Internet Protocol (TCP/IP) the most commonly used protocol for Internet communications. Router-based firewalls control traffic at the IP level going into or coming out of the internal network, blocking or passing along data packets depending on the packet's header. They examine the network application service requested (e.g., FTP, Telnet protocol type, e.g., Transmission Control Protocol User Datagram Protocol (ICMP), and the source and destination address of each packet that arrives at the firewall. The network administrator configures the packet-filtering firewalls to accept or reject packets according to a list of acceptable hosts, routes, or services.

Unfortunately, when a firewall is reading these packets, network performance may slow down by as much as 20%. Other drawbacks of router-based firewalls include:

- The firewalls do not allow for granular control of the packets.
- They are cumbersome to code and when set up incorrectly may offer a false sense of security.
- They usually do not log the actions that take place at the firewall, so the network administrator cannot monitor how hackers are attempting to break into the system.

**Host-Based Application-Level Firewalls**

Host-based application-level firewalls are considered more flexible and more secure than router-based IP-level firewalls. They reside on a host computer, typically a dedicated UNIX machine, PC, or Macintosh and can be configured to support elaborate network access control policies with fine granularity. Application level-firewalls control network application connections (e.g., Telnet, FTP, SMTP down to the individual or group level by type of action and time of action permissible. The ability to limit the time when certain functions run is particularly useful, because many renegade hackers, dubbed midnight hackers, work late at night and network administrators need to be able to restrict many of the potentially unsecured Internet functions during those hours.

One of the essential features of the application-level firewall is that it allows the network administrator to monitor a log of activities that take place at the firewall. This log can be used to identify potential breaches of security and to monitor resource usage.

A recent rash of network break-ins has been accomplished by IP-spoofing. IP-spoofing takes advantage of the UNIX OS, which erroneously presumes that anyone who logs in to a server using a previously approved TCP/IP address must be an authorized user.
By altering the source IP, someone can spoof the firewall into believing a packet is coming from a trusted source. To combat this problem, many firewalls reject all packets originating from the external network and carrying an internal source IP.

Secure Interfaces

The secure interfaces level of security is rather sophisticated, somewhat akin to installing a new form of support beams in a house. Secure interfaces are software programs that allow for additional security checks in the network interface. Several companies offer these interfaces, most of which work with the various Web browsers as well as with Web server software. The most common secure interfaces are Netscape Communications Corp.’s SSL (secure sockets layer) and SHTP (secure hypertext transfer protocol).

SSL

SSL sits between TCP/IP and HTTP or other protocols such as Simple Network Management Protocol or FTP. It provides privacy, authentication, and data integrity. MCI is one of the largest SSL users, employing the interface in InternetMCI. Other users include First Data Card Services (the world's largest credit-card authorization firm), First Interstate, Old Kent, Bank of America, Norwest Card Services, as well as MasterCard International.

S-HTTP

S-HTTP extends HTTP to allow both the client and the server to negotiate various levels of security based on public-key encryption and provides encryption, authentication, and digital-signature features. It can also distinguish the origin of a particular document on any server. It was created by Terisa Systems, a joint venture between RSA Data Security and Enterprise Integration Technologies. S-HTTP’s strengths include its availability and flexibility.

Both the SSL and S-HTTP have been competing to become the standard secure interface for commercial sites on the Web. To head off the competition, Terisa Systems released a developers' tool kit supporting both standards. Many other secure interfaces also exist, each with its own set of features.

Legal Issues

Many companies overlook the potential legal issues associated with connecting to the World Wide Web. The press has focused attention on many of these issues, including the availability of child pornography, bootlegged software, and ease of infringement of copyright laws. IS managers should be aware of these potential dangers and take measures to protect employees and enterprises from lawsuits and loss of valuable copyrighted data.

This layer of security is comparable to household plumbing, which allows for unwanted items to be flushed away. For example, if FTP access to the server is allowed, network administrators should consider either prohibiting external users from placing files on the server or frequently purging files off the server. This guards against unwanted guests using the server as a clearing house for pirated software.

One well-publicized case of such an incident occurred at Florida State University, where unknown individuals employed a seldomly used computer as a storage facility for pirated software. It is not implausible that the owners of the server may be found liable for
what resided on the computer, regardless of whether they had knowledge about it, and be brought to court on copyright infringement charges.

To curb access to sexually explicit materials, many companies are restricting access to a variety of UseNet groups. Although this practice may cut off the source of some illicit materials, users have other ways of gaining access to such materials. Companies cannot monitor the actions of all employees, but they may be able to reduce the likelihood of access to inappropriate sites by educating employees on what type of behavior will not be tolerated and aggressively enforcing such stances.

Employees also need to be educated on copyright laws. Although it is fairly well known that copying commercial, nonshareware, computer programs is illegal, other forms of copyright infringement are less obvious. Downloading a copy of a favorite song or distributing an article found on the network without permission may violate copyright laws.

Companies need to be concerned not only with what employees obtain but also with what they post outside the company. Employees may unwittingly release strategic information over the Internet, thereby jeopardizing data or potential profits. The only way to guard against such situations is through employee education that also encourages people to contact their IS manager, in-house counsel, or network administrator when they have questions.

Conclusion

The field of security and the threats to a corporate network will always be changing. The first step IS managers can take to secure a corporate network is to understand the range of security issues associated with Internet and Web access. The desired level of security must then be determined and security measures implemented.

Security needs to be viewed as a holistic process, because it is only as strong as its weakest link. Remaining aware of new developments in the field and continually adjusting security measures is one way of meeting the changing risks inherent on the Internet.

Some of the more recent yet still uncommon developments include HERF guns (high energy radio frequency guns) and EMPT bombs (electromagnetic pulse transformer bombs). Both of these threats can wipe out an entire data center, and the only way to be protected from them is to put corporate servers and data sources underground and secured in heavy paneling.

By monitoring server logs, staying alert to new security hazards, and altering the security system as needed, companies may be able to deter unwanted guests from visiting the corporate network. Organizations must also have adequate back-up plans that speed up recovery from the potentially devastating damages resulting from a successful security breach.

Author Biographies

Monica J. Garfield

Monica J. Garfield is a doctoral student in MIS at the University of Georgia in Athens. As a former technical assistant with the Mitre Corp., she worked on the AWACS radar program.

Patrick G. McKeown