

How does your online payment security measure up?

The security breaches that disrupt service, destroy privacy and corrupt information have become part of the lore of Internet security and not infrequently, a favorite topic for the media. But in spite of the headlines, the way we do business is increasingly based on inter-dependencies and electronic links – a seeming conundrum unless you take into account the effective security measures deployed by the leading financial institutions.

Today, with companies of every size and description forming globe-spanning e-business relationships, the security of online banking has become a growing concern. The major financial institutions have met this challenge on two levels—first with an ongoing investment in sophisticated systems and software to establish effective safeguards, and second by engaging their clients as active partners in the security process.

Today, with companies of every size and description forming globe-spanning e-business relationships, the security of online banking has become a growing concern

What follows is a series of basic security measures to use as a yardstick for your own company's relationship with your online banking provider. As we examine each of these measures, including authentication, encryption, system contingency, network security and intrusion detection, as well as an overview of your own responsibilities, you may find yourself discovering that security is truly a process – and wondering how your own online banking provider deals with these issues.

Authentication: Establishing who can access your account

The first line of defense in any online system is to establish who is or is not an authorized system user in order to limit entry to the system. The historic "protection" once provided by one or two static passwords has now evolved into a dynamic process that puts up multiple barriers to entry. For example, for users who handle transactions,

many systems require the use of a "token," or interactive device, which generates a dynamic password that is then entered in the system. Since dynamic passwords are never repeated, it greatly reduces the risk of unauthorized access.

For users who handle repetitive processes but are not involved in transaction initiation or approval, secured passwords, set to expire every 30 days, may be used in conjunction with the employee's "regular" ID number.

As you probably know, most systems set a limit on the allowable number of bad entry attempts. Once a user is locked out, the resetting of passwords should be handled by written request only, signed by your authorized security manager. In the event that an authorized user leaves the company, his or her profile should be automatically deleted from the system. Even when the dynamic password token is not turned in, this will ensure that it is permanently disabled – eliminating the possibility of unauthorized use.

Encryption: Mathematical codes for protecting sensitive information

Encryption or coding has been in use for centuries – long before the first computer was invented. However the ability of the computer to quickly generate long and complex "keys" has raised the effectiveness of encryption to unprecedented levels. Keys are the fundamental element in generating modern cyphertext. A key is a particular value which, when applied to plaintext, encrypts it and when applied to cyphertext, allows the message to be decrypted. The greater the number of bits, or the longer the key, the more difficult it is to break the encrypted message. The current standard is 128-bit encryption – and the odds against someone cracking such a code are staggering -- only 1 in 1 septillion.

Obviously, you want to be sure that your payment data be protected with no less than 128-bit session level encryption. However, if your global payments are limited by government restriction to only 40-bit encryption, be sure your online banking provider uses server gated cryptography that can upgrade a browser from 40-bit to 128-bit encryption.

When sending payments, the 128-bit secure socket link (SSL) that resides in your browser should be automatically invoked at the beginning of the session, when the user connects to the server. Should you have the need to encrypt files delivered out of session, they can be protected by S/MIME, a secure, multipart Internet mail extension.

System Contingency: How to prepare for or avoid a crisis

A loss of function, whether the result of a temporary power interruption or longer-term damage, can have far-reaching effects on a company's reputation and ability to do business. The best defense is to make sure that your service provider has put the necessary safeguards in place: system architecture that is designed to provide full off-site contingency with back-up and recovery sites; duplicate components at both the primary and secondary sites including multiple applications servers as well as Web servers, utility servers and database servers. As a further precaution, annual contingency testing should be conducted on all system components.

Network Security and Intrusion Detection: Ensuring against unauthorized entry to the system

The critical importance of the Web server is probably best described by its location between the external and internal firewall, an area referred to as the De-Militarized Zone (DMZ). In this context, it should be protected by multiple levels of defense, beginning with the management of the firewalls, which have state-of-the-art intrusion detection capabilities that should be continuously monitored. An external firewall allows incoming traffic only through designated ports and an incoming firewall protects the applications servers against intrusion. Another level of defense is the management of user privileges and entitlements on the Web server, which should be handled by a dedicated independent unit. Finally, there should be continuous upgrades to the servers in order to close any newly detected vulnerability gaps as well as the use of anti-virus software to protect servers, desktops and PCs.

Encryption or coding has been in use for centuries – long before the first computer was invented

One of the most effective defenses against intrusion has been to fight fire with fire, through the use of "ethical hackers." These are bonded companies that are paid to deliberately attempt to hack into networks and look for vulnerabilities in new applications, prior to their release. If your provider utilizes ethical hackers, you may want to find if the relationship with the ethical hacking company is controlled at a high corporate level, and whether any findings during this process are resolved and reviewed by internal IT groups, before an enhancement goes into production.

On the Client Side: Defining your own responsibilities

Although the greatest single advantage of Internet delivered cash management is the high level of control at the client site, it is a way of life that requires constant vigilance. Your authorized Security Manager is the gatekeeper. He or she sets up the user profiles that allow employees to access specific applications and functions of the bank system – based on the limits that you determine. For example, one group of users may be authorized to download files only, but not to initiate transactions. Another group may be restricted to the number and type of transactions, on specific days in a one-month period. In addition, there should be maker/checker control to prevent unauthorized payments. To validate a particular user's authorized responsibilities, your security manager should have access to a variety of audit reports that review and monitor user activity. In summary, there should be safeguards in place at every step of every secure process to guard against the possibility of human or systematic error.

One of the most effective defenses against intrusion has been to fight fire with fire, through the use of "ethical hackers"

Evaluation and Decision

If you are concerned about e-payment security, these basic issues can serve as a yardstick for evaluation – or as a discussion guide for use in meetings with your online banking provider. Ultimately, security is fundamental to the electronic conduct of business, and should guide the selection of your online banking provider. The advantage to working with the largest banks is that they have the resources and the operational structure in place for ongoing system development. The one you choose should not only demonstrate the ability to address your particular needs, but also display a commitment to building a long-term relationship with your company – which in the long run, is the basis for ongoing security.

Roman Kadron, a Senior Vice President with Citibank, is the Citibank e-Business Group Information Security Officer. One of his main responsibilities is to oversee the security of CitiDirect® Online Banking, the bank's flagship Internet-based transaction services system for corporate clients. For more information, contact Roman at roman.kadron@citigroup.com or visit www.citidirect.com.

