Global Transaction Banking
A Passion to Perform.
Deutsche Bank
Spring 2007

INSIGHTS FROM CASH MANAGEMENT, US
TreasuryPulse

Mitigate Online Fraud Risks with Holistic Approach to Security

Corporations conducting business online face the threat of fraud and theft each day. Creative Internet-based schemes try to compromise corporate security by corrupting your computers, luring you to reveal financial or personal information, and in some cases capturing sensitive data in a transparent fashion.

Companies and their service providers must stay ever vigilant to secure their computer systems and online transactions against the variety of sophisticated schemes used today.

"Phishing" is one such scheme. It involves an unsolicited e-mail made to look as if it's from a legitimate source. A phishing e-mail contains a malicious attachment or a link to a fake web site that asks for personal identification information. According to the Anti-Phishing Working Group, the number of phishing spoof sites reached an all-time high of 29,930 in January 2007, an increase of 25% from the previous month.

Using "keystroke logging" or "keylogging" software, criminals can capture and download passwords, IDs, account information and other sensitive data that you or other employees have keyed into your computers. These applications are often distributed through "Trojan horse" software that can be downloaded and installed on a computer without the owner's permission or knowledge.

Malicious software code called "malware" can infiltrate your computer, server or network by exploiting existing security weaknesses. These viruses, worms and Trojan horses quietly enter through e-mails, instant messages, web sites and file downloads—and proceed to damage your computer system.

Take a Holistic Approach
It's important to take a holistic view of your security policy and validate it on a periodic basis. Companies also need a thorough understanding of their applications in order to assess and mitigate the risks they present.

Unauthorized transactions can occur internally as well as externally, so be sure to look inside your organization to find areas of vulnerability that might compromise your company's information. In addition, carefully scrutinize your online interactions with outside service providers and vendors. Hold providers accountable for ensuring that the data you provide them remains secure.

The following are some measures you can consider building into your security policy and procedures:

- Document all processes and audit them on a periodic basis.
- Require secondary approval on payments exceeding certain dollar limits.
- Segregate duties. Assign two different people to initiate and reconcile payments.
- Keep user access, IDs and passwords updated. Stale or dormant accounts are prime targets for fraudsters.
- Conduct frequent, periodic housekeeping to keep your organization's information up to date.
- Never click on web links in unsolicited e-mails.
- Ignore e-mails requesting account information or other confidential data. Legitimate providers will not seek sensitive data in this manner.
- Validate the access rights that are established with your providers. Ask providers how they secure your information, such as using firewalls and anti-virus software.
- Ask your own organization the same security questions you ask of your service providers on a yearly basis to continue improving your defenses.

Multifactor Authentication

Meanwhile, regulators and the banking industry are stepping up efforts to secure online financial transactions. The Federal Financial Institutions Examination Council (FFIEC) issued guidance in October 2005 recommending multifactor authentication to banks as a better way to mitigate risks related to such transactions, and banks have been responding.

Multifactor authentication affords layered security. It requires an additional method of authenticating a user besides the standard ID and password. This method usually takes the form of an image or physical item.

Another form of authentication involves a provider monitoring a user's usage patterns and behavior. Any behavior that falls outside an acceptable range of a person's typical usage patterns is flagged for further authentication. For example, your provider may detect that your user ID is logged in from two physically different locations or different countries, and would pursue an investigation into the matter.

Deutsche Bank uses layered security throughout its db-direct internet online cash management portal and modules. For clients who desire a hardware-based layer of security, the Bank offers the option of using a smart card or token device for user authentication when accessing the web site. Deutsche Bank further secures transaction initiation by requiring the use of a smart card device during transaction approval.