

HOME
BANKING
ECONOMY
FINANCIAL PLANNING
FROM THE REGULATORS
INSURANCE
INVESTMENT DEALERS
MARKETS
MUTUAL FUNDS
PEOPLE
WHAT'S ON

FEATURES

TODAY'S MUST READ
ASK THE EXPERTS
FUND MANAGER FORUM
OPINION POLL

DEPARTMENTS

ABOUT US
BACK ISSUES
CAREERS
CLASSIFIEDS
LINKS TO INDUSTRY
CUSTOMIZE E-NEWS
SEARCH THE SITE
(Advanced Search)
SUBSCRIBE TO
INVESTMENT EXECUTIVE
SUBSCRIBER SERVICES

CURRENT ISSUE

Technology

Passwords are passe

Industry increasingly to rely on biometric technology to protect data

September 2001

BY Donalee Moulton

For the past decade, financial analysts and brokers have relied heavily on password protection to keep prying eyes from sensitive and confidential client data. However, time and again, passwords have proven they're not foolproof. That's why the financial sector is passing over this form of security in favour of the next generation of electronic protection — biometrics — which relies on physical characteristics such as fingerprints and retinal scans.

There are a number of problems with passwords. First, they are easily forgotten. Second, passwords are easily decoded. Most computer users pick a simple password, one they think will be easily remembered. "Passwords are easy to break. People are inherently lazy," says Robert Lendvai, vice president of marketing with **Kyberpass Corp.**, an Ottawa-based software security developer.

Forgetfulness and easy pickings come with a price. Michael Dodgson, product manager, commercial notebooks, with **Compaq Canada Inc.** in Toronto, says up to half of all calls to help desks are password-related. The more password-heavy the organization, the higher that number.

Companies are also under surveillance from peeping Toms — whether they know it or not. A survey of 500 companies conducted by the U.S. Federal Bureau of Investigation found 90% of companies reported having security-related problems in the previous 12 months — about one-third of them came from within the company.

A survey of Fortune 1000 companies conducted by Pinkerton, a California-based security firm, found that Internet and intranet security issues took second place on the Top 10 list of security concerns. "The potential for theft of trade secrets and customer information, damage to sensitive data and interruption of commerce presents unprecedented vulnerability to businesses," says Pinkerton president Don Walker.

That threat is especially significant for financial services firms. "[But] companies can protect themselves from attack,"

Does the disclosure of executive compensation benefit shareholders?

EDUCATION
2001

Continuing Education
Center

Bissett Funds
IT'LL CHANGE MORE
THAN YOUR PORTFOLIO

AIC
GROUP OF FUNDS

IE HIGHLIGHTS

Chasing the rabbit
Motivating clients to remain invested and focused on their financial plans is a challenge. But if you can get them to keep their eyes on the prize and stay invested, you can retain assets and build long-term, rewarding relationships with them

Call for higher limits
Retirement coalition says increase is

says Lendvai. "Financial companies tend to be at the higher end of the protection spectrum."

Use of Biometrics to rise

The increasing use of biometrics is expected to decrease dramatically the cost of in-house password management, while tightening security, protection and privacy.

There are two primary types of biometrics on the market: fingerprint readers and retinal scans. Neither technology is groundbreaking or new.

What have changed are the size and the cost of these tools. As technology advances, the size and complexity of fingerprint and retinal readers has decreased significantly. As a result, there's more use.

According to **IDC**, a Massachusetts-based technology research firm, the biometrics market is expected to hit US\$1.8 billion in the next three years, up from US\$166 million two years ago.

At present, fingerprint scans are eating up about 47% of the biometrics market. This is primarily a reflection of cost and accessibility. In 1998, Compaq was first off the mark with a fingerprint reader that attached directly to the desktop. Last year, the company released a biometrics PC card for mobile personal computers. The cost of a fingerprint reader, which can handle up to eight different fingerprint images, is about \$260.

The portable reader works like this: a tiny camera converts an image of a fingerprint into a "map" that cannot be duplicated. The map is then encrypted and stored in the computer. Accessing information is a snap, says Dodgson. "Users simply apply their fingerprints and off they go." What is not simple is replicating the fingerprint image, he adds. "There's no way for [someone] to circumvent the fingerprint. Our fingerprints are unique."

With retinal scans, an image of the user's retina is encrypted and stored. To access information, a user's retina is scanned and compared with the stored image. A perfect match unlocks the system.

Two problems are holding back the widespread use of retinal readers — cost and safety. This technology, now estimated to have about 15% of the worldwide biometrics market, costs about \$3,000. There's also concern about the effect repeated use of laser scans might have on the eye.

Electronic signatures confirm identities

Doing business online requires some way of proving customers are who they say they are and companies are who they purport to be. "Without the ability to authenticate online, the transaction must go offline at some point," says Robert Lendvai, vice president of marketing with **Kyberpass** Corp., an Ottawa-based software security firm.

Electronic signatures can provide the necessary identification, keeping transactions online. These signatures usually involve a twofold process: private encryption technology allows the sender to sign a document, then public encryption technology lets the signature be read and

long overdue

Parked funds

\$52 billion is sitting in money market funds, but how much will go to equities

Options now 51% of CEO pay

verified.

Underlying the use of electronic signatures is public key infrastructure — PKI — which lets users digitally sign and authenticate and allows for real-time verification.

According to research firm IDC, the total market for PKI products and certificate authority services will grow at a rate of 61% compounded annually, to US\$3 billion in 2004 from US\$281 million in 1999. "PKI technology is moving from pilot testing into the real world of e-commerce," says Charles Kolodgy, research manager for IDC's internet security program.

"New deployments of PKI technologies, including remote access, secure messaging, content delivery and transactional security, demonstrate the technology's transition from the test track to the production roadway," he adds.

The next generation is an Internet banking solution called iBanking that is powered by PKI security on a smart card. iBanking is designed to provide financial services and investment customers with a full range of banking services.
IE

E-mail this article to a friend or associate

E-mail your comments to the author of this article

Copyright © 2001
All Rights Reserved.