View from the Top: Banks and security

September 13 2005

The world's leading banking executives gathered last week in Copenhagen, Denmark, for the SIBOS tradeshow, a slick and well-attended annual meeting sponsored by banking network provider Swift. While most businesspeople have likely never heard of Swift, they are in fact a stunningly important part of the world banking system: Nearly every inter-banking transaction, from fund transfers to asset swaps, takes place over Swift's private banking network.

The Brussels-based company is launching its next-generation network, and bankers agree Swift's conservative approach and the fact that the Swift network is exclusively private to banks and large corporations make it a safe place to conduct financial business.

Not so, however, with that "other" network, the Internet.

It's been a tough year for bankers as Internet identity theft left millions of their customers exposed through break-ins and "phishing" scams, in which e-mails are sent by scammers to unwary consumers asking for personal information. In the first half of 2005, six major U.S. financial institutions reported customer-information theft, either through employee theft, database break-ins, or in one instance a simple case of lost delivery. In this instance, an overnight-delivery service failed to deliver a data backup tape containing sensitive customer information, leaving the financial giant no choice but to publicly disclose the loss and the potential threat to its customers.

While the mood among the bankers in Copenhagen had brightened considerably since those dark days in early 2005, there is a determination among them to take greater steps in protecting customer information. Encryption technologies for protecting customer data have existed for some time, though the banking community -- particularly in the United States -- has been slow to adopt them. The higher cost of providing protection had previously forced most U.S. banks to avoid employing those protections for their customers. Now, however, after the high-profile break-ins and pending federal legislation, they may have no choice.

Congress is currently considering a number of data-protection bills that will force U.S. companies to protect consumer information. The bill considered most likely to pass is Senate Bill 1408, sponsored by John McCain of Arizona and Ted Stevens of Alaska, among others. In the current draft of that bill are hefty penalties for any company that fails to protect its consumer information. Versions of the bill have even included jail time for executives of those companies, though most followers of the legislation believe it will be considerably watered down by the time that it is passed.

In addition, identity theft for bankers has had a major deleterious effect on their business: Recent studies show that online banking in the United States is on the decline. That, along with the looming threat of federal regulation, has led to the many renewed pledges by the bankers to end identity theft, though the solutions may seem as complex as the problem.

Bankers are therefore taking a fresh look at the vast array of protection technologies that verify the end user and encrypt sensitive data. The verification of the end user is crucial to a bank knowing that the consumer who just logged in is who they claim to be; encryption technologies scramble data so that it can only be read by those who have the proper decryption key. Both are critical to better data protection for banks.

The first challenge, verifying the user's identity, can today be provided in a number of ways: The oldest technique is using a One Time Password ("OTP") generator. This device is a small plastic token with a face screen that displays numeric passwords every 30 seconds. A computer at the bank knows what the valid number that user should be entering is at that exact moment, and thus allows the user to enter the network.

Corporations have used this technique for their traveling employees for years, but the costs are high and users don't like having to fumble between the OTP device and the computer to input this information. Two newer devices are the USB token, a thumb-sized device plugged into the USB port of a computer that contains a digital certificate identifying the end user. The other is the Smart Card, a credit-card sized token that plugs into a special reader in the computer. It also contains a digital certificate, and newer cards come with biometric thumbprint readers for added security. There are also new software programs that encrypt databases, so that employees and outsiders cannot get to the information unless first authenticated through endpoint identity devices like USB tokens and Smart Cards.

Either way, expect to see your bank provide a choice of strong authentication, and expect your employer and your federal government to someday do the same. Identity theft challenges all of your identities, and proving who you are will only grow as a way of life.

Chris Fedde is senior vice president and general manager of Enterprise Security Division at SafeNet, the seventh-largest global leader in information security. Fedde has been a key contributor to building the company's security presence in the federal government and the financial community. Fedde holds a BSEE degree from the University of Iowa.

Citation: View from the Top: Banks and security (2005, September 13) retrieved 24 April 2024 from https://phys.org/news/2005-09-view-banks.html