

What are you doing about two-factor authentication?

Jay Cline

July 6, 2006 ([Computerworld](#))

If you work for a financial institution or a company that processes credit card transactions, this isn't news to you: There's a growing push to require two-factor authentication for logging into your company's information systems.

But if you're in this camp, you're probably also finding out how expensive and operationally challenging it is to require users to remember a password and also some other mechanism, such as a plastic token, to log in successfully. National attention on two-factor authentication is generating as much hype as network intrusion detection and stored data encryption did a few years ago.

Not sure which authentication approach is best for your company? Then it's probably time to take a step back and reassess the alternatives.

What exactly are the new requirements? In January 2005, the payment-card industry issued the now-famous PCI Data Standards. Among the many PCI standards, which apply worldwide to companies that process payments using Visa, MasterCard, American Express or Discover cards, was this nugget: "Implement two-factor authentication for remote-access to the network by employees, administrators, and third parties."

Later, last October, the Federal Financial Institutions Examination Council (FFIEC) weighed in on the topic. The FFIEC, which creates the standards for federal audits of U.S. financial institutions, issued guidelines stating that "single-factor authentication, as the only control mechanism" was "inadequate" for Internet-based products and services such as online banking.

With these two mandates, what was once wishful thinking by hardened security professionals has now entered boardroom budgeting discussions across the country. But just what is two-factor authentication?

Security professionals have traditionally defined it this way: choosing something you know — usually a password — along with either something you have, such as a cardkey, or something about who you are, such as your fingerprint. The idea behind this approach is that it would be virtually impossible for a criminal to simultaneously be in possession of two of these types of authenticators.

This is where theory runs up against some hard reality. Password management already chews up huge amounts of IT resources, with password resets accounting for roughly a third of help desk inquiries in many companies.

Add to this the prospect of implementing new hardware and software on employee laptops to handle cardkey swipes or fingerprint scans, or requiring customers to always carry on their keychains another card or token, and suddenly you're facing an enormous financial and operational undertaking. The impact is often big enough for companies to ask if the reduced risk from two-factor authentication is worth the cost.

If traditional approaches to two-factor authentication are taken, what could be the corporate impact? First, companies may decide to greatly reduce the number of employees with remote access into the network. Instead, they'll restrict most employees to remotely access only their e-mail through a Web application such as Outlook Web Access. It simply may be too expensive to grant remote-network access as a default privilege. The result of employees not being able to get to their files on the network may be lost productivity.

Second, banks could start charging customers to use online banking to pay for the increased administrative costs of two-factor authentication. Customers would probably welcome this as much as they did the chance to pay ATM fees. The result could be fewer online banking customers.

Some privacy and security leaders I've spoken with say these costs and operational challenges are making it time to step back and reassess the situation. They're asking two main questions:

- What risks are we actually trying to mitigate with these new regulations?
- Are there other ways, besides traditional two-factor authentication, to combat these risks?

The standard answer to the first question has been simple: that the purpose of the second factor of authentication is to compensate for the weaknesses of the first factor, the password. Weak passwords can be cracked with free software available on the Internet; they can often be discovered inside files stored on the network or people's laptops, or on sticky notes left inside desk drawers; and they can be solicited through social engineering and phishing e-mails.

These are serious risks that could expose a company to a publicized security-breach notification, often a multimillion-dollar affair. But are there other sufficiently effective and cheaper ways to compensate for weak passwords?

My counterparts point to a few possibilities:

- Challenge questions. Who says you always need to choose from two of the three categories of what you know, what you have and who you are? Why not choose two authenticators based on what you know? If you can choose the right set of challenge questions — such as "What is the high school you graduated from?" or "What is your favorite pet's name?" — you can counter some of the weaknesses common to passwords.
- Photo "passwords." This is another variant of a second "what you know" authenticator. In this method, you choose a photo — either of yourself, or something memorable you choose from a gallery — that will be associated with your account. Each time you log in, you face a random selection of photos that will always include the one you originally designated, which you must choose correctly.

- "Bingo" cards. This authenticator is a form of "what you have." They're wallet-size grids that resemble bingo cards that you receive when you set up your account. When you log in, the system will randomly generate coordinates, such as Row B, Column 5. The cell at that coordinate will have a PIN that you enter.
- Fraud detection. Instead of adding a second authenticator, it may be more cost-effective to strengthen your fraud-detection measures, looking for anomalies based on IP address, geographic location or other behaviors inconsistent with the user's past patterns.

Security professionals will differ on which authenticators they think are right for their organizations. But they'll all agree on one point: it's bad for business and bad for the economy for standards organizations to mandate a one-size-fits-all solution. Continued flexibility is the right way to go to address this complex risk.

Table 1: Two-Factor Authentication: No Silver Bullet		
Companies trying to reduce the risk of fraudulent account takeovers face many options, but none that is cheap, convenient and secure at the same time.		
Authenticators	Pro	Con
Something you have...		
Keycard or smart card	<ul style="list-style-type: none"> ■Somewhat convenient - user carries it in wallet with other credit cards ■Can be integrated with an employee ID badge 	■Expensive - requires new hardware and software
Token with PIN	■Somewhat convenient - user carries it on a keychain	■Expensive - requires new hardware and software
Token inserted in the USB port	■Somewhat convenient - user carries it on a keychain	■Expensive - requires new hardware and software
Digital certificate	■Convenient - stored on the user's laptop	■Somewhat expensive - requires new software, and the user is tied to that computer
"Bingo" cards	<ul style="list-style-type: none"> ■Somewhat convenient - user carries it in wallet with other credit cards ■No new hardware 	■Somewhat expensive - requires card distribution and some software enhancements

Something you are...		
Fingerprint scan	<ul style="list-style-type: none"> ■Very convenient - the user can never forget it or lose it 	<ul style="list-style-type: none"> ■Expensive - requires new hardware and software ■Not 100% accurate
Something you know...		
Photo "passwords"	<ul style="list-style-type: none"> ■Very convenient - no extra cards or equipment to carry around. 	<ul style="list-style-type: none"> ■Somewhat expensive - service licensing and software enhancements
Challenge questions	<ul style="list-style-type: none"> ■Very convenient - no extra cards or equipment to carry around ■Inexpensive 	<ul style="list-style-type: none"> ■Not as foolproof as other methods. May need to have multiple challenge questions.

Jay Cline manages data privacy at Carlson Companies Inc., a Minneapolis-based group of businesses in the travel, hospitality and marketing industries. Contact him at cwprivacy@computerworld.com. These are his views and not necessarily those of Carlson, and should not be taken as legal advice.