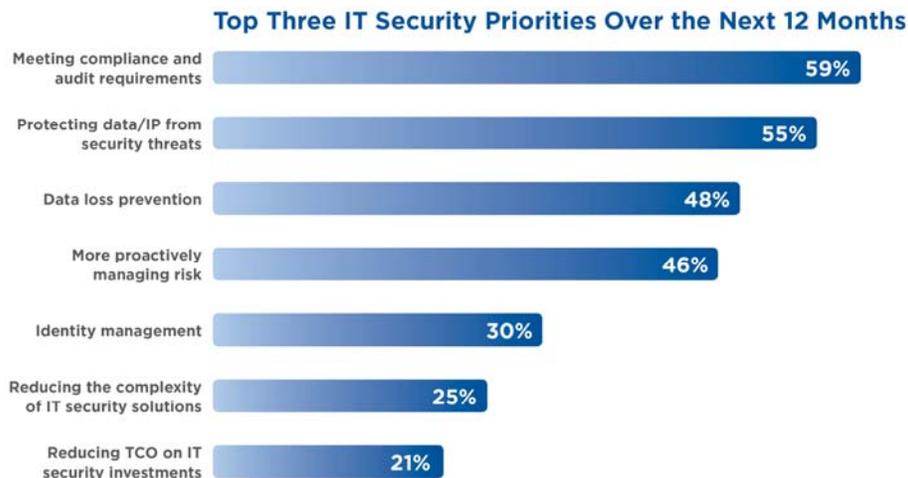**HID**®

Take the cost, complexity and frustration out of two-factor authentication

Combine physical and logical access control on a single card to address the challenges of strong authentication in network security

Organizations of all sizes are struggling to implement and enforce strong security without raising costs, increasing the management burden on IT and impacting user productivity. No longer can this issue be brushed aside as most industries now have data protection standards and compliance requirements that must be met.

A July 2010 CSO magazine Market Pulse study found that 93 percent of the IT leaders surveyed feel pressured to improve enterprise security due to increased risk. These risks come in the form of internal and external threats.

That said, their three main focus areas for the coming year are 1) meeting compliance requirements, 2) protecting intellectual property and 3) preventing data loss. They agree that two-factor authentication could be a key enabler to help them achieve these goals. Still, many are reluctant to deploy this stronger form of authentication due to cost, complexity and the burden on users to carry yet another item, such as a token or a USB device.

Top Three IT Security Priorities Over the Next 12 Months

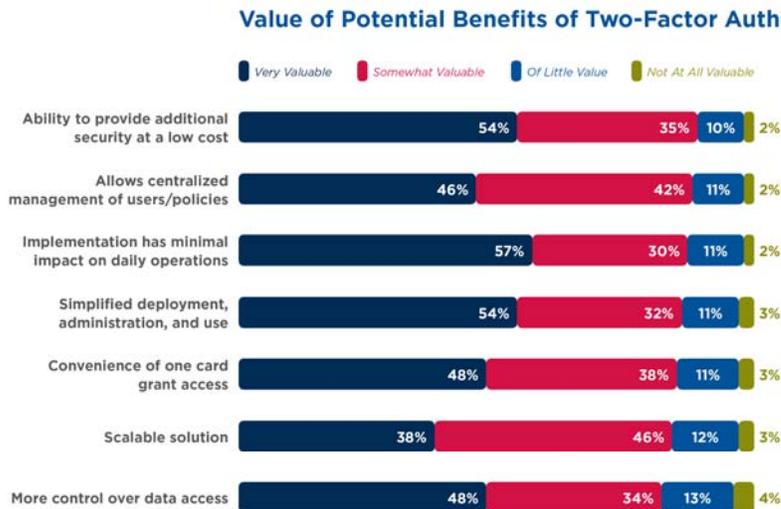| Priority	Percentage
Meeting compliance and audit requirements	59%
Protecting data/IP from security threats	55%
Data loss prevention	48%
More proactively managing risk	46%
Identity management	30%
Reducing the complexity of IT security solutions	25%
Reducing TCO on IT security investments	21%

Source: IDG Research Services, July 2010

HID Global addresses these concerns by placing building (physical) and network (logical) access control on a card already in use as an identity badge to gain access to an organization's buildings. The HID on the Desktop™ solution—comprising access control cards, OMNIKEY® contact and contactless card readers, and naviGO™ management software—provides a cost-effective, user-friendly solution for a strong security posture.

HID on the Desktop provides varying levels of risk-appropriate security solutions to suit an organization's risk tolerance and budget. For instance, card technology ranges from basic two-factor authentication using the card and a PIN to a higher level of network security that uses Public Key Infrastructure (PKI) and digital certificates.

HID extends an organization's existing card-based access control system to network security, offering a simple, convenient option for two-factor authentication that is affordable, reliable and secure.

IT's pressure cooker

If there's one clear result from the CSO study, it's that IT leaders are aware of the need for heightened security. As noted above, the vast majority, reflected by their survey responses, know they have to boost network security to handle the increased volume of threats coming at them.

Value of Potential Benefits of Two-Factor Authentication

Legend: ■ Very Valuable ■ Somewhat Valuable ■ Of Little Value ■ Not At All Valuable

Benefit	Very Valuable	Somewhat Valuable	Of Little Value	Not At All Valuable
Ability to provide additional security at a low cost	54%	35%	10%	2%
Allows centralized management of users/policies	46%	42%	11%	2%
Implementation has minimal impact on daily operations	57%	30%	11%	2%
Simplified deployment, administration, and use	54%	32%	11%	3%
Convenience of one card grant access	48%	38%	11%	3%
Scalable solution	38%	46%	12%	3%
More control over data access	48%	34%	13%	4%

Source: IDG Research Services, July 2010

Another factor that is forcing them to confront security head-on is the rise in regulatory and compliance requirements—92 percent of respondents agree this is making the landscape more challenging.

At the same time, 91 percent of respondents reported that IT security technology is becoming more complex. The conclusion that can be drawn from this data is that although IT leaders are under the gun to do better in terms of protecting their networks, vast and complicated security architectures are proving too cumbersome to manage and maintain.

As an example of how this complexity is thwarting their efforts to address security, in the past 12 months, 47 percent experienced escalating costs of user access and 45 percent had difficulty auditing the environment due to fragmented systems.

Despite such obstacles, a majority of IT leaders surveyed identify their top objectives for the next 12 months as meeting compliance requirements (59 percent), protecting data and intellectual property (55 percent), and data loss prevention (48 percent).

Stepping up security

Until now, many companies have used baseline security, such as username and password, to control access to data and many will continue to settle for this out-of-the-box solution. Unfortunately, this will most likely have disappointing results.

The inherent weakness of username and password systems is commonly known. In 2006, Microsoft co-founder Bill Gates, in his keynote address at an RSA Security conference, pointed to username/password systems as a significant security problem. "Another weak link is

authentication," Gates said. "Today, we're using password systems, and password systems simply won't cut it; in fact, they're very quickly becoming the weak link."

The problem with username and password systems starts with the concept of a username itself. Most follow a simple format such as the user's first initial and last name so that they are easy to remember. Unfortunately, this simplicity makes them easy to guess by hackers. That leaves only the password as a means for protecting access to an organization's data.

Many IT administrators allow users to choose their own password. But the onslaught of password cracking tools, keystroke loggers, network monitoring tools and brute force attacks has forced IT to take more control over this process. In addition, passwords can be stolen via shoulder-surfing (where someone looks over a user's shoulder) or through social engineering such as phishing scams.

Some organizations allow users to share logins and passwords. This approach is risky as it does not enable IT teams to track and audit individual user activity while enforcing role-based policies for internal and external users in order to meet government and industry standards.

To combat this problem, IT issues guidelines that require users to each have their own login and password. They also demand the use of "strong" passwords that include numbers or special characters. Some have instituted policies that increase the length of passwords or force users to frequently change their passwords. All of these methods produce the unintended consequence of passwords being written down on sticky notes or scraps of paper. By trying to enhance security, IT has wound up negating password "secrecy" and compromising network safety.

Getting "smarter"

The potential for compromised security that username and password systems present is addressed head-on with two-factor authentication. Two-factor authentication requires users to provide something they have, such as a smart card, and something they know, such as a PIN. Even if the PIN is compromised, without the card as the other factor, authentication is impossible.
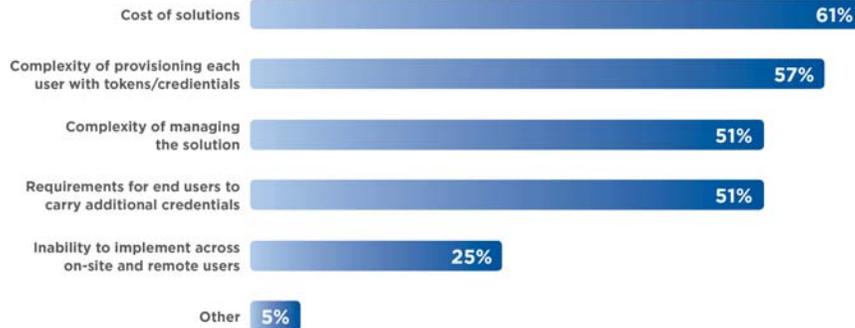
Gates warned that the password problem was bound to get worse as more passwords are needed. He lauded what he called "multi-factor authentication." "We need to move in the direction of smart cards, and multi-factor authentication must be built into the system itself. We need the ability to track what goes on and have a built-in recovery system," he told the RSA attendees.

The solution to the problem that Gates lays out lies in two-factor authentication, which represents a much more complex security model, making it difficult to bypass or spoof. However, it's a method that is familiar to users. It resembles the ATM model where a user presents a card to a machine and enters a PIN to gain access to his account.

Among the CSO survey respondents, 61 percent say that they have not implemented strong authentication, but believe it would help them meet their top objectives.

So, if they're convinced that two-factor authentication is the path to a stronger security posture, what's standing in the way? Just over 60 percent of the survey respondents cite cost, 57 percent point to the complexity of provisioning tokens and credentials, 51 percent note the complexity of managing the solution and 51 percent cite the burden on users to carry yet another item with them, such as a token or USB device, as a barrier. A full 25 percent note the difficulty of implementing two-factor authentication across on-site and remote users.

Top Challenges/Barriers Associated with Implementation

Challenge	Percentage
Cost of solutions	61%
Complexity of provisioning each user with tokens/credientials	57%
Complexity of managing the solution	51%
Requirements for end users to carry additional credentials	51%
Inability to implement across on-site and remote users	25%
Other	5%

Source: IDG Research Services, July 2010

In essence, for organizations to get onboard with two-factor authentication the solution must be simple for the user and not disrupt productivity; easily and affordably scaled as the user base grows; simple for IT to deploy and administer; and provide a way to meet regulatory and compliance demands across the entire organization.

Alleviating two-factor authentication concerns

HID on the Desktop does all of this by leveraging the physical access ID cards that more than 75 percent of the respondents say they already have and use on a daily basis. Organizations are accustomed to provisioning and managing these cards, and users are accustomed to carrying them, facilitating the transition to two-factor authentication on laptops and at the desktop.

In fact, just over a third of IT teams are unaware that they can extend their physical access control solution to network access control, according to the CSO Market Pulse study. However, they do see value in such a system. An overwhelming majority,

88 percent, see the value in such a solution to provide additional security at a low cost. They also value the fact that a converged card solution that provides both physical and logical access allows centralized management of users and policies, that implementation has minimal impact on daily operations, and that it provides simplified deployment, administration and use. Finally, they appreciate the fact that it's scalable, provides ability to audit data access and offers convenience by having one card grant access to offices, desktops and networks.

All of these value propositions led 7 in 10 respondents to say that they were likely to consider a converged two-factor authentication solution like HID on the Desktop.

Depending on the risk level required by the organization, HID on the Desktop provides various risk-appropriate solutions. For instance, organizations highly concerned about security can use HID's Crescendo smart cards, which are PKI-enabled. Just below Crescendo is iCLASS, a contactless smart card. iCLASS secures the session with encryption and mutual authentication. Finally, users looking for a simpler, yet still strong, two-factor authentication strategy can make use of the widely deployed Prox contactless smart card.

Risk-Appropriate Approach to Two-Factor Authentication
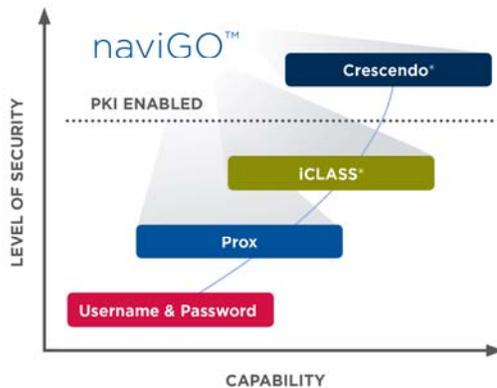
All of these options, which fall on a continuum of strong authentication security, are far more secure than username and password.

Self service security

All HID cards work in conjunction with HID's OMNIKEY contact or contactless card readers, available in a variety of form factors to suit the needs of nearly any application. naviGO software reads a user's card and requests his/her PIN. If the user can't remember that information, he or she is provided an emergency portal that features steps to securely retrieve it via knowledge-based authentication (KBA). This self-service approach eliminates the need for IT to get involved and reduces the cost that can be incurred by password resets in terms of IT time and loss of user productivity.

Organizations can also use HID on the Desktop to set and enforce automated centralized access policies for on-site and remote users. These policies tie into Microsoft's ActiveDirectory via naviGO so organizations can easily track and audit individual user activity to comply with industry and government mandates.

As we pointed out earlier, an overwhelming majority of survey respondents—some 88 percent—recognize the significant benefits of leveraging existing physical card access systems in a two-factor security environment.

HID on the Desktop is an easy and affordable solution to increasing security in your organization and meeting regulatory and compliance demands. Now is the time to act to create a highly secure data environment with the convenience and cost-effectiveness of the HID on the Desktop solution.