

PRESS CONTACT:
Belinda Banks
S&S Public Relations
(609) 750-9110
belinda@sspr.com

FIVE REASONS WHY MULTIPLE PASSWORDS AREN'T PRACTICAL (AND WHY SINGLE SIGN-ON ISN'T THE ANSWER)

FAIRFAX, VA — (9/24/2008) — No one disputes that passwords are essential for protecting enterprise networks and applications. Past that point of agreement, however, things get murky very fast.

Some IT professionals believe that passwords are a relatively simple security matter. No password management policy is necessary, and employees are bright and responsible enough to handle their password obligations. Unfortunately, two major realities come into play:

1. **Employees are drowning in passwords.** To paraphrase the famous potato chip slogan, “Bet you can’t use just one.” In its November 2007 survey by Siber Systems of over 600 U.S. IT professionals, conducted through business data company eMedia, over 75% of respondents reported that their employees are required to remember from three to as many as ten passwords to do their daily tasks. One or two passwords, it seems, simply aren’t enough.
2. **Diminishing security returns.** Many employers require workers to change their passwords on a regular basis, or they introduce new security gateways requiring fresh passwords. Trouble is, as the number of passwords goes up, effectiveness actually decreases. Multiple passwords invite user fatigue, rule breaking, and overuse of help desks for assistance in resetting lost passwords.

Such concerns are why Single Sign-On (SSO) was invented. SSO is an additional security software layer applied on top of an enterprise’s applications and network resources. By logging into the SSO system using a single password, the user gains authenticated access to all their digital tools.

While it’s true that SSO only requires employees to remember one password, the technology invites other problems that plague IT staffers. The top three are:

1. **Expensive, time-consuming implementation.** To install SSO, IT workers must assemble all passwords being used by employees—a formidable task even for mid-sized companies. They must then configure the SSO system to implement all the log-in protocols for each digital resource.
2. **Single point of attack.** Because everything “password” now resides in one place, it creates the perfect target for hackers who want to unlock any, or all, system resources.

- more -

Five Reasons Why Multiple Passwords Aren't Practical (And Why Single Sign-On Isn't The Answer)—Page 2

3. **Issues with partner sites.** It's not always possible to configure SSO systems for use with third-party or partner systems. Such situations are on the increase, especially with the growth of collaborative and interconnected computing.

Distributed Solution

Amid this difficult situation, a third alternative is available that solves the problems of both SSO and "hands-off" password management. RoboForm Enterprise, from Siber Systems, is a distributed, client-side software "vault" that securely stores multiple employee usernames, passwords and other confidential information using powerful AES encryption and a user-defined master password.

Winner of PC Magazine's Editors Choice award and recommended by the New York Times, The Wall Street Journal, C|NET, Morningstar and other top organizations, RoboForm quickly pays for itself through faster implementation and fewer help desk calls. What's more, the flexibility and distributed architecture of RoboForm Enterprise ensures that there are no "keys to the kingdom" that will allow phishers, keyloggers or hackers to compromise an enterprise's password storehouse.

RoboForm Enterprise is compatible with most automated software install programs, making it easy to deploy on hundreds or even thousands of PCs. Administrators can also fully customize every feature to meet specific corporate security and password standards. The solution not only creates a near-immediate ROI, but also improves employee morale because only one master password is required.

For more information about RoboForm Enterprise visit www.roboform.com/enterprise; for a free copy of Siber Systems' survey report entitled "Password Management Survey: IT Managers Respond to Password Security Challenges Facing Today's Corporations," go to www.roboform.com/enterprise/download/survey.html.

About Siber Systems:

Founded in 1995, Siber Systems creates and markets a wide range of software to both professional programmers and the general public. The company's three best-known products are RoboForm, RoboForm2Go, and GoodSync. RoboForm, a unique password manager and identity organizer for PCs and mobile devices, has over two million active users worldwide and is available in both consumer and enterprise versions. RoboForm2Go is a portable version of RoboForm that runs directly from USB flash drives combining convenient and secure password management with complete portability. GoodSync is a powerful, yet easy-to-use file backup and synchronization software. The firm also licenses various data parsing, compilation, and transformation products to major technology companies. Headquartered in Fairfax, Virginia, Siber Systems is privately held.

###