

Password Management Survey

**IT Managers Respond
to the Impact of Password Policies
on Security and Productivity**





Overview

A growing trend for many companies is to implement stronger password policies designed to increase network security. Employees in companies from across all industries find themselves having too many passwords. This trend has forced help desks to constantly field requests for password retrieves and resets, causing a waste of time and valuable resources. In addition, many companies find new password policies only exacerbate their problems and lead to decreased security, increased user frustration, and low employee morale.

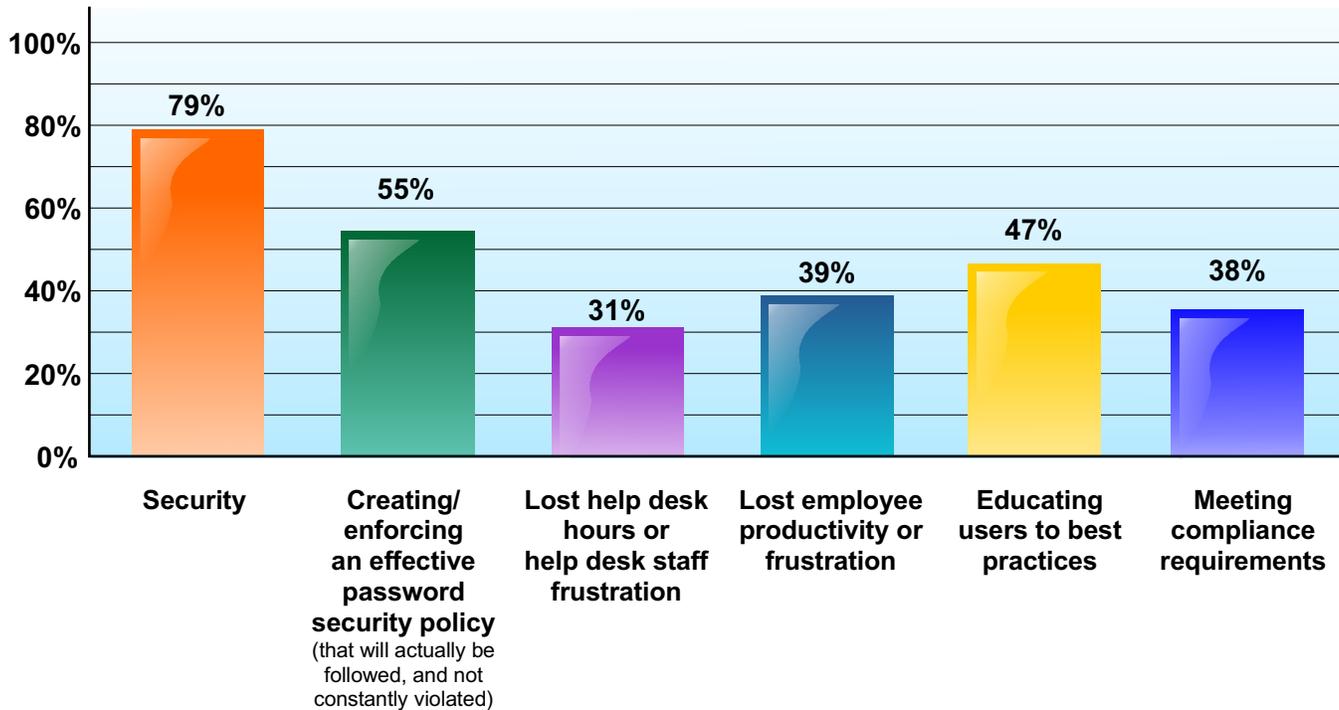
In November of 2007 Siber Systems and eMedia conducted a survey in which 600 IT professionals were asked a series of questions about password security, password convenience, as well as current challenges related to password management in their respective organizations. The questions ranged from "What are your primary password management concerns?" to "What percentage of calls to your IT staff consist of password-oriented requests?"

Professionals of all levels and disciplines were represented across many different industries. Executives with titles of Chairman, CEO, President, Principal, Owner, or Vice President accounted for 12% of all respondents. Almost 25% held titles of CIO, CTO, Director, or Security Officer. Close to 30% of respondents were either a Manager, Senior System Administrator, or System Administrator. Engineers, Analysts, Architects, and Developers made up 22%. The remaining 11% held titles of Consultant, Coordinator, Professor, Scientist, Dean, or CFO.

This report summarizes major findings and shows how RoboForm Enterprise, an award-winning password management solution by Siber Systems, can increase corporate security, eliminate password related help desk calls, improve end user productivity and convenience, and decrease overall IT costs.



Q: What are your primary password management concerns?



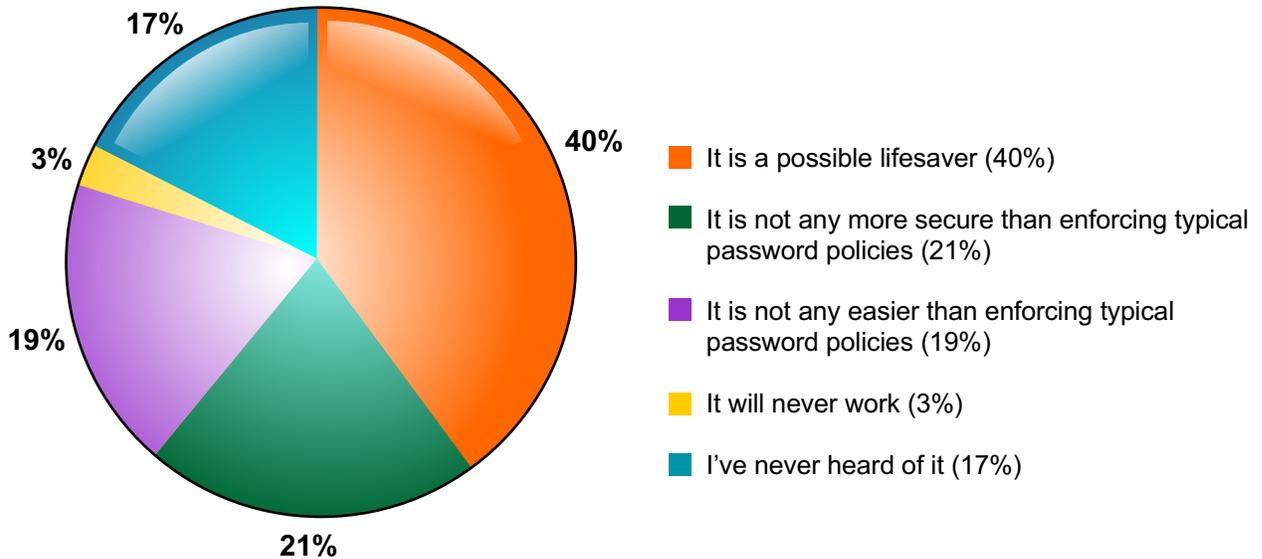
Summary Results

As one might expect, the primary password management concern of IT professionals is security. Yet it is interesting to note the strong showing of other concerns, such as creating a policy that users will actually follow, the need to educate users on best practices, and the lost productivity and user frustration that passwords (and strict password policies) often cause.

RoboForm Enterprise Addresses All Concerns

RoboForm Enterprise is a password management solution that addresses all of these primary concerns. It offers enhanced security by allowing users to sign on to all password-protected sites with a single, strong password. RoboForm Enterprise users only memorize one Master Password, allowing the software to manage access to all web-based services.

Q: What do you think of the concept of a 'Master Password'?



Summary Results

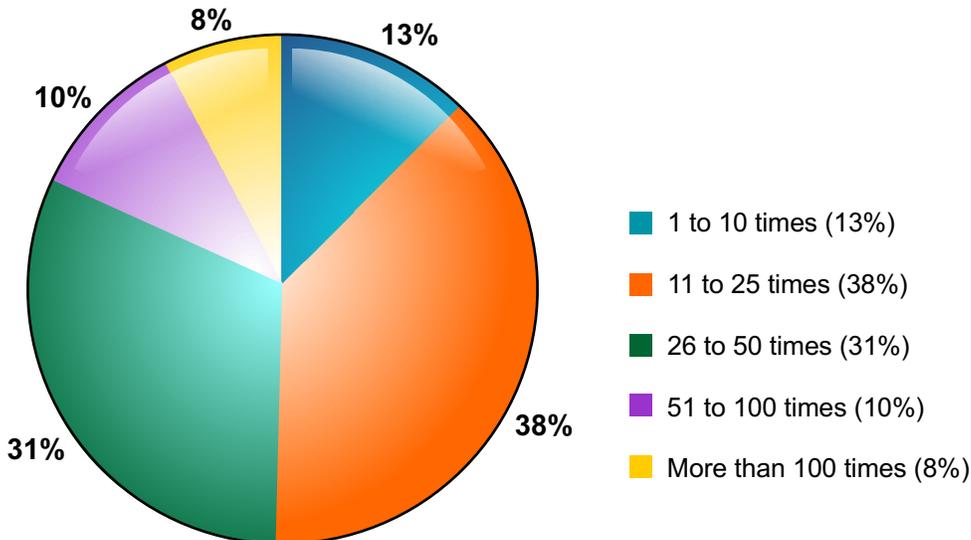
A Master Password is one strong password that an employee uses to log into a program which can automatically manage all other passwords for this user's accounts.

The concept of the Master Password recognizes that users can only be reasonably expected to remember a few passwords. After all, how many strong passwords can a user remember? With all the network logons, email accounts and web-based services a typical user confronts, the answer is "not many," which is why 40% of respondents said that a single "Master Password" that manages access to all password-protected sites and services "is a possible lifesaver."

RoboForm Enterprise Reduces Many Passwords to One Secure Password

RoboForm Enterprise users log in once using a secure "Master Password," allowing the software to take care of the rest, securely storing and managing usernames and passwords for other login-required services. It is also intelligent enough to protect against phishing scams as it will not provide login credentials to phony sites.

Q: How many times during a workweek does an average employee use company-required passwords?



Summary Results

49% of survey respondents estimate that their users have to use company-required passwords at least 26 times a week. When users have to authenticate this often, anything that makes the process easier for them will increase productivity and make for a happier workforce. Power users typically average more than 100 logins per week.

IT professionals want to keep resources secure, but it's asking a lot to expect regular network users to memorize and use strong passwords as often as the survey results indicate. In that kind of environment it's inevitable that users will take shortcuts. They'll...

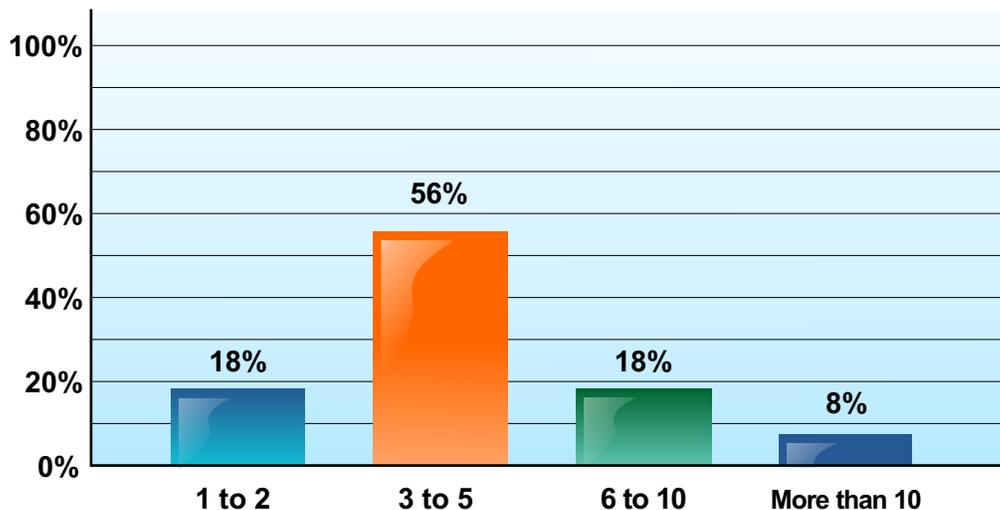
- Write down passwords in an insecure location
- Use the same password for several different accounts
- Share passwords with co-workers
- Use passwords that are easy to remember, but are also easy for someone to guess or for software to crack

Simply establishing a strong password policy won't increase security. In fact, a strong password policy by itself is likely to result in more users taking shortcuts, thus decreasing security and increasing user frustration.

RoboForm Enterprise Increases User Productivity and Security While Decreasing User Frustration

RoboForm Enterprise manages all logins, allowing IT departments to insist on a strong password policy without expecting users to remember multiple strong passwords, something they most likely won't do anyway.

Q: How many passwords is an average employee in your organization expected to remember?



Summary Results

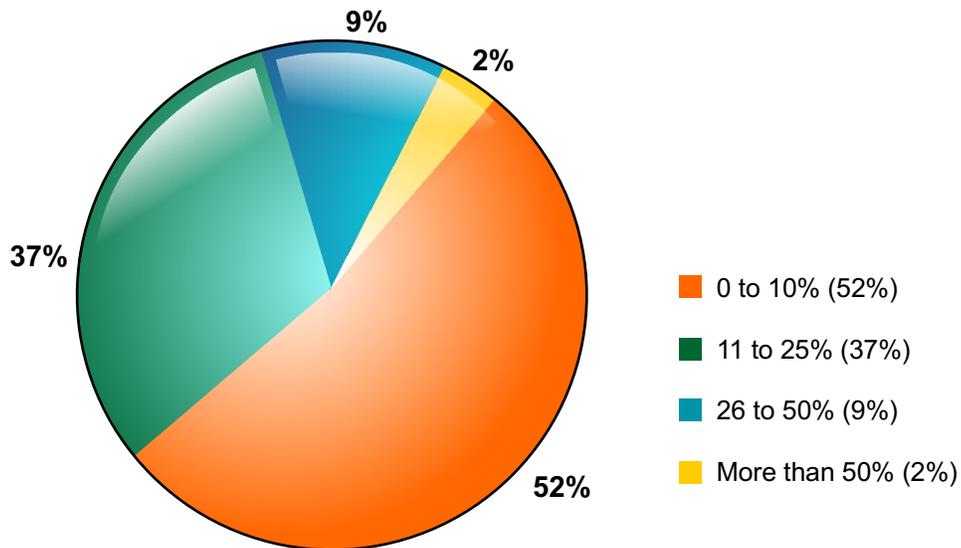
The simple fact of the matter is that users are asked to remember too many passwords. A whopping 83% of respondents said that users on their system have to know at a minimum of three passwords.

As a side note, the number of usernames and passwords required may prove to be underreported, since (based on personal interviews) a sizable number of IT professionals answering this question seemed not fully aware of other passwords that employees required.

The RoboForm Enterprise Solution

RoboForm Enterprise allows users to select one secure password and then the software manages all the other secure passwords necessary for other sites and services. Since RoboForm Enterprise remembers and securely stores these usernames and passwords, they can be strong, alphanumeric passwords, and can be different for every website or application.

Q: What percentage of calls to your IT staff consist of password-oriented requests?



Summary Results

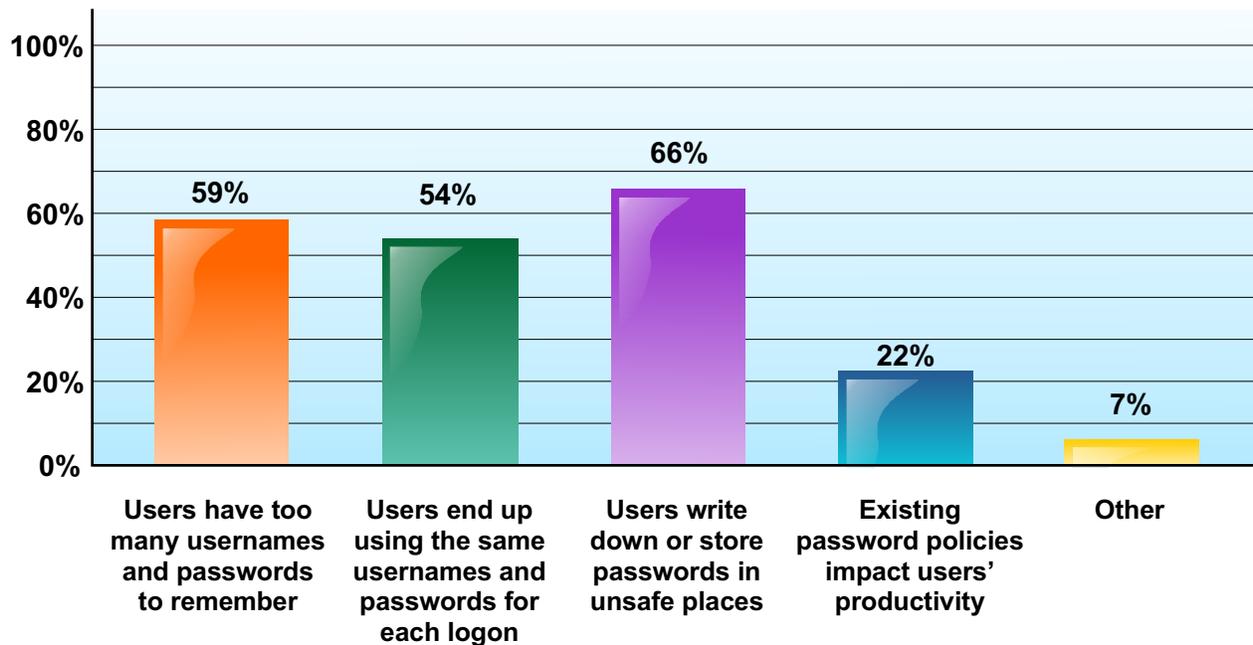
Almost half of those surveyed reported that at least 11% of IT staff time is spent dealing with password-related requests. These results show the extent of the problem, and the potential cost-savings of a password management solution like RoboForm Enterprise.

It should be noted that we believe the actual percentage is much higher. CIOs, IT Managers, and System Administrators (those with more intimate knowledge) reported significantly higher percentages of password-related calls than Chairmen, CEOs, and Presidents.

RoboForm Enterprise Will Reduce Your IT Costs

In many cases, the low costs associated with deployment of RoboForm Enterprise will be quickly recovered by help desk savings alone. This makes RoboForm Enterprise a smart choice for any corporate environment.

Q: What immediate password problems are you seeking to solve?



Summary Results

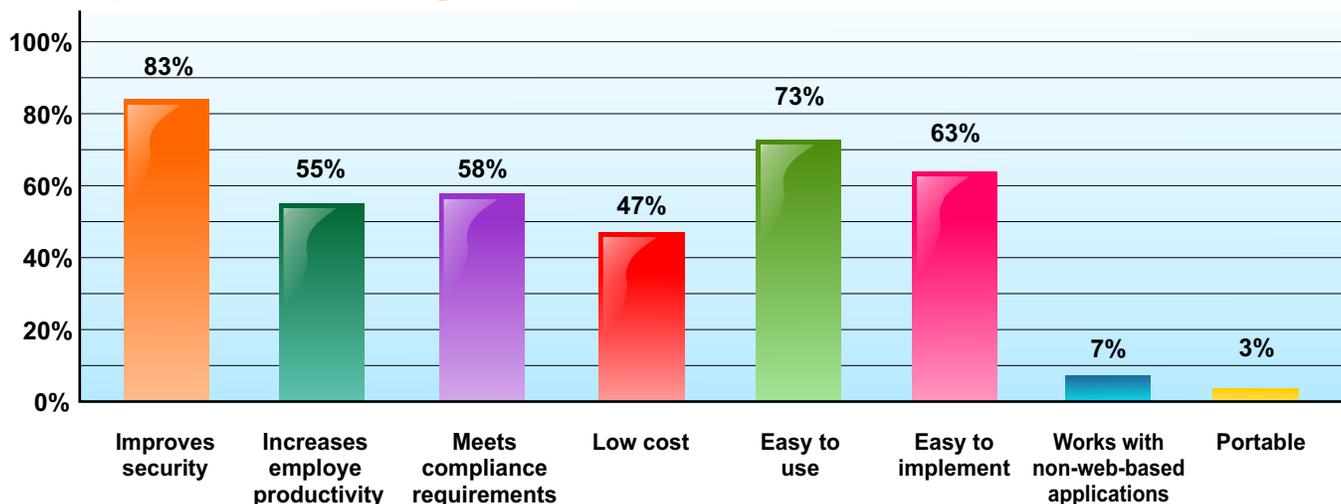
66% of respondents report the old "yellow sticky note" problem. Faced with too many passwords to remember, users will write them down in insecure locations, many times right next to their computer. The results above also demonstrate that the "yellow sticky note" is not the only password related issue, as a typical IT department faces many other password management challenges as well.

Can we really blame the employees? It's unreasonable to expect users to memorize multiple strong passwords. In addition, they're not as concerned about security. They are more interested in productivity and ease of use.

RoboForm Enterprise Increases Password Security and Productivity

One of RoboForm Enterprise's advantages is that it only expects the user to memorize one strong password. Once the user authenticates with RoboForm Enterprise, the software securely manages all network and web logins. It can be customized to meet company security and compliance requirements, relieving some of IT burden, and making life easier for employees.

Q: Which features are most important to you regarding a password management solution?



Summary Results

IT professionals know the value of a strong password policy, but they also know the frustration of trying to enforce such a policy on users who don't feel that they are directly responsible for hacked networks, compromised passwords, or other password related issues. The results show that improved security, ease of use, and ease of implementation are the most important features in a password management solution.

IT professionals need a way to enforce a strong password policy that users will actually follow, and that's precisely what RoboForm Enterprise provides.

RoboForm Enterprise is a Complete Solution

The RoboForm Enterprise list of features described below meets and exceeds the requirements of survey respondents.

Improves Security: RoboForm Enterprise encrypts and saves user passwords on the user's machine only, and autofills passwords to login forms. It's also able to generate secure passwords for an additional level of security.

Increases Employee Productivity: RoboForm Enterprise users only need to remember one secure password, which gives them access to all the sites and services they need to use. This creates an ideal situation where IT can have its strong password policies, users don't have to remember too many passwords, and the help desk isn't swamped with password-related requests.

Meets Compliance Requirements: RoboForm Enterprise makes it easy to enforce strong password management policies throughout an organization, meeting the most stringent security compliance requirements.

Low Cost: RoboForm Enterprise is a very affordable product for most organizations, one that easily pays for itself in the time it will save reducing password-related help desk calls and increasing employee productivity.

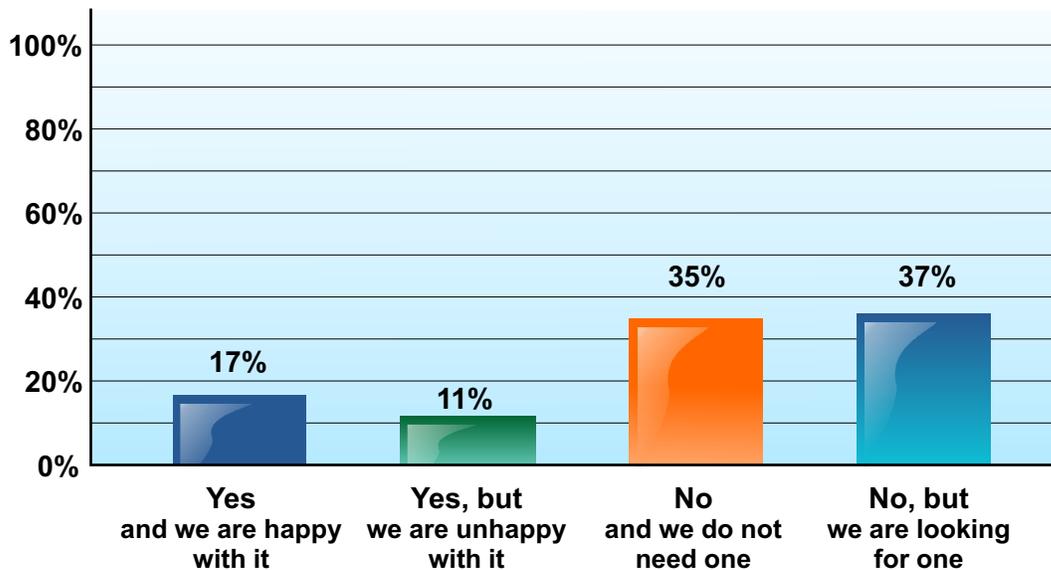
Easy-to-Use: RoboForm Enterprise users log in once, and the program manages all their password requirements. It even completes online forms, and works with IE, Netscape, Mozilla, Firefox, and more.

Easy-to-Implement: IT managers can completely customize RoboForm Enterprise to meet enterprise security requirements in less than 15 minutes.

Works with Non-Web-Based Applications: RoboForm Enterprise manages passwords for every type of login your users will confront, whether its network, web, or application-based.

Portable: Users can take RoboForm Enterprise with them on a USB device, sync passwords, with a Palm or Pocket PC, back up and restore, or print passwords.

Q: Do you have an existing password management solution?



Summary Results

Despite the clear need for a password management solution only 17% of respondents have a solution they're happy with. Consequently 48% of companies are currently struggling with this issue, what's alarming is that 35% feel they don't need a password management solution at all.

Nevertheless, based on these results, it's apparent that at least half of all responding companies are having difficulty in finding a solution that is a right fit for their organization.

RoboForm Enterprise is the Right Solution for You

If you want to stay current with the security issues faced by your colleagues, you owe it to yourself to get familiar with the RoboForm Enterprise solution.

Overall Summary

Due to the growing number of online and offline applications that require username and password logons, more than a third of companies surveyed plan to implement a new, or improve an existing password management solution before the end of 2008.

Top reasons offered for implementing a new solution/improving an existing one emphasized the need to improve security, have a solution that is easy to implement and use, as well as one that increases the productivity of both help desk staff and the rank and file employee.

The majority of IT professionals indicated that while they need to, and are seeking to make their work environment more secure and productive, they are also focused on complying with corporate and government regulations.

Despite the increased emphasis on password management, only 17% report that they both have an existing password management solution and are happy with it.

Conclusion

Many organizations currently struggle with password management issues. RoboForm Enterprise lets companies implement a low-risk (try before you buy), cost-effective, easy, and secure password management solution. It will meet and exceed the expectations of even the most demanding IT professionals, as it is easy to implement, user-friendly, and pays for itself in cost savings and increased productivity.

For more information about RoboForm Enterprise, visit www.roboform.com/enterprise.

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 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 a USB flash drive 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.