Enterprise Password Management

A Best Practices Guide for Solving the Fallout of Password Inflation

Using RoboForm Enterprise to Increase Password Security, Improve Employee Productivity and Decrease IT Costs

Release Date: May 4, 2007

Table of Contents

Executive Summary

The Goal: Increase your corporate IT password security.

The Problems: The helpdesk gets more calls that tie up the IT department, employees store passwords in insecure files or simply write down their passwords.

Password inflation and the password fatigue that comes with it increasingly frustrate not only end users but also the support teams that deal with the fallout of strict password polices.

Power users and even rank and file knowledge workers have to deal with scores of passwords. There are simply too many usernames and passwords to remember, or, the length and complexity of each password hinders a productive work flow. Therefore, employees often violate prudent password standards.

Since more business-critical data is being made available online, balancing end user convenience and effective security and password policies is more important than ever. Company executives have to balance the free-flow of information against the nightmare of a major security breach.

The Solution: RoboForm Enterprise is an advanced, full-featured—distributed—password management solution that:

- improves security
- increases employee productivity
- decreases IT and support costs, and results in
- an immediate Return on Investment.

RoboForm Enterprise remembers your employees' passwords, securely stores them on their computer, logs them into web applications automatically, and completes forms with one click. RoboForm is very powerful and many of your power users may already be using and benefiting from a personal copy of our consumer version of RoboForm.

RoboForm Enterprise is a better, easier, and more cost-effective solution than multi-factor authentication or enterprise single sign-on.

- Our easy and pain-free installation process does not require a huge integration effort like most other Enterprise products.
- In less than 15 minutes you can customize RoboForm Enterprise to meet your company's strict password policies.
- RoboForm Enterprise can be tested before mass deployment, and provides a low-risk, real password management solution.
- Perhaps the most important benefit is that employees will actually use this tool-and will never want to go back to their old ways.

This white paper:

- describes appropriate password standards,
- explores the potential negative consequences of "password inflation,"
- contrasts the various methods of dealing with Enterprise Single Sign-On (SSO), and,
- describes an alternative approach to SSO (RoboForm Enterprise).

Introduction: Using Passwords is an Essential Security Technique Employed to Restrict Access to Secure Networks, Web Properties and More

Passwords are absolutely essential to restrict access to valid users. Unfortunately, our list of passwords keeps growing. It's now common for a typical computer user to have 20 to 30 different passwords, or more.

The Conundrum

There are several well-known and generally accepted standards to effective password management.

1) Passwords must be a least 6-8 characters long.
2) Passwords should never be a common word found in the dictionary and should contain at least one letter and one digit. Even stronger passwords should contain at least one punctuation mark or special character.
3) Passwords should contain a mix of upper-case and lower-case letters.
4) Passwords should be changed every 30 days.

Unfortunately, as passwords and strict password management has become more important, employees have become less careful. Remembering several passwords is difficult. Employees take shortcuts, making personal information and digital identities less secure.

This significantly increases corporate security risks.

Common Employee Short Cuts

It's hard for people to remember complicated passwords, many different passwords, frequently changing passwords and/or seldom used passwords.

As a result employees typically:

- Forget their passwords, which requires numerous calls to the helpdesk to retrieve or reset their passwords.
- Write down their passwords or store passwords in insecure files on their computer, which reduces the effectiveness of a secure password.
- Rely on the browser, cookies, or an unsecured web site to remember their passwords.
- Use simple and easy to remember passwords that can be easily compromised.
- Recycle and reuse combinations of the same passwords.

All of these typical employee shortcuts compromise security for obvious reasons.

Techniques to Create Strong, but Easy-to-Remember Passwords

It's imperative that a company adopt a policy of strong password management practices.

One approach is to offer special training sessions to teach employees some simple techniques, described in more detail below. Of course, this approach assumes that after the training and encouragement to use stronger passwords, the employees actually follow through.

A good password is

- a combination of letters and numbers that cannot be found in a dictionary
- at least 6 to 8 characters long
- free of any personal information such as your name, child's name, occupation telephone number, address or birth date
- a combination of letters, numbers and symbols
- a mix of capital and lower-case letters

Perhaps the single most important thing to remember when creating a new password is make the password hard to guess, but easy to remember. That's easier said than done, but by following the guidelines below you will start using passwords that are more secure than what you're using now.

There are several techniques you can employ to make your existing passwords more difficult for hackers to crack. Whatever method you choose you should remember to make it an easy and understandable method so you will have stronger passwords without much more effort.

Acronym Method - Use the first letter from every word in your favorite expression, or line in a story, poem or movie. For example, “Pay no attention to the man behind the curtain,” could lead you to the following password: PnAttMBtC.

Number Substitution - Choose a word as your password, but then substitute similar looking numbers for letters in your passwords. For example, Football may become “F00t8a77” or sneakers may become “5n3aK3r5”. Here is a sample list of numbers that could be substituted for letters:

O…0
I …1
Z…2
E…3
H…4
S…5
G…6
L…7
B…8

You don't need to associate every number with a letter. What is important is that you remember your list of associated letters and numbers.

Keystroke Technique - Choose a password that you want to use and then come up with a keystroke mapping system. For example, if you choose to do an “upper-left” keystroke system you would choose the letter to the upper-left of the actual key you wanted. So if your password was “qwert” (not recommended) your new password would be “12345” (also not recommended). If the word you wanted to use for your password was football, your keystroke password would be “r995gqoo”. It sounds complicated, but you need to look at your keyboard anyway, why not just choose the letter to the upper-left, left, or lower-right of the word you choose to remember.

Companies Face Significant Security Risks and Threats

Identity theft was the most-reported complaint to the Federal Trade Commission in 2004, up 15 percent from 2003 to 247,000 complaints. The problem has intensified because of the speed and availability of information on the Internet, and as we need to remember more usernames and passwords to access various accounts, we are becoming increasingly less careful when choosing our username/password combinations.

Identity thieves are primarily focused on getting your passwords. Once the culprits collect your passwords, they gain access to your accounts, steal your identity and use the information for personal benefit.

A strong password policy can help, but it doesn't prevent three very common security risks: phishing, password hacking, and keylogging.

Phishing is a widespread form of Internet piracy that "fishes" for your personal financial information account numbers, Social Security number, passwords, etc. Thieves use this confidential information to run up bills on your credit or debit cards, take out loans or even obtain a driver's license in your name.

Password hacking commonly occurs by guessing people's passwords based on personal information, or by “brute force” through the use of password hacking software.

Keylogging software is a tool used to capture a user's keystrokes. It can be used to determine usernames, passwords, and other personally identifiable information and is widely available on the Internet.

These attacks pose significant risks to companies. Imposing strict password requirements won't solve these problems, and sometimes it only creates more, as employees take shortcuts and may actually create a bigger problem.

To find an appropriate and enforceable balance, organizations need to look carefully at their password policies, understand the affects of password length, complexity and aging requirements on users.

Multiple Security Options Available

Companies have several options available and must determine their best solution based on several factors, including costs, time to implement, and needs. Three of the most common solutions to increase password security are:

- Multi-factor Authentication,
- Enterprise Single Sign-On, or
- Adopting strong password policies.

Multi-factor Authentication

Multifactor authentication means there are at least two different types of credentials that must be submitted to be authenticated. There are three categories of authentication factors:

- something you have (a hardware or software token),
- something you know (a password), and
- something you are (a thumbprint, retina scan or voice print).

Each factor in the authentication mechanism should be from a different category.

By layering on additional factors in your authentication process, you make it very tough for hackers to force their way into your systems.

Enterprise Single Sign-On

Enterprise Single Sign-On (ESSO) is an authentication mechanism that enables a user to authenticate once and gain access to the resources of multiple software systems.

Many companies promote ESSO, but ESSO solutions often take months, if not years, to deploy across an enterprise, require extensive application integration, and typically do not provide an immediate ROI.

Strong Passwords

Given the inherent complexities and significant costs associated with multi-factor authentication and ESSO, most companies attempt to solve their password challenges by simply adopting and attempting to enforce stricter password management policies. The problem with this solution, as mentioned previously in the paper, is that it is inherently difficult for your employees to meet the standards necessary to create a secure environment. This generally leads to employees taking other shortcuts that compromise security, or significantly increased calls and costs to the IT department.

RoboForm Enterprise–Your Best Practices Approach to Secure and Easy to Use Password Management

An effective enterprise password management solution can have a major impact on your business. When determining your password policies, remember that most users are capable of remembering one relatively strong password without writing it down, so using a single, strong password to access many different websites often represents the best long-term solution.

RoboForm Enterprise is specifically designed to quickly and effectively address your most immediate password management concerns. It allows your organization to use stronger password management practices without compromising security or increasing costs.

To address the password-related problems and challenges outlined throughout this white paper, RoboForm Enterprise provides the following capabilities.

Encrypted Passwords

RoboForm securely stores employee usernames, passwords and other confidential information on their computer using powerful AES encryption. When an employee visits a password-protected website, RoboForm automatically retrieves their data and logs them in with one click.

Only One Password to Remember

All passwords and other important information are protected using a Master Password. So a user remembers one Master Password and RoboForm remembers the rest.

True One-Click Logins

RoboForm's powerful technology allows employees to login to web sites automatically. Simply select any RoboForm Passcard and RoboForm will:

a) Navigate to the web site
b) Enter your username and password
c) Click the submit button . . . all in one click!

Automatically Completes Long Web Forms

Filling long forms has never been easier. With RoboForm your employee simply clicks on their Identity and RoboForm will complete the entire form.

Protects Your Company Data

Since RoboForm will remember all passwords, your employees can now use hard-to-guess passwords for all your logins. RoboForm comes with a secure password generator to improve password security. RoboForm also protects your employees from Keyloggers and Phishing scams.

RoboForm Enterprise Key Features

Policy Editor
Using the Policy Editor system administrators can “freeze” and customize various features of RoboForm Enterprise to align with company password standards.

Easy to Use
Employees remember one password, RoboForm remembers the rest.

Saves Time
Automates logins to websites.

Saves More Time
RoboForm completes long forms with one click.

Secures Your Information
Stores passwords on your employees’ computers and protects them with powerful AES encryption.

Strengthens Passwords
Generates secure passwords to increase password protection.

Fights Phishing
Matches each username/password pair only to authentic sites.

Defeats Keyloggers
Bypasses the keyboard so there's nothing to log.

Improves Password Organization
Backs-up, prints and easily organizes your passwords.

Increases Search Capabilities
Enables easy search on any website from the RoboForm toolbar.

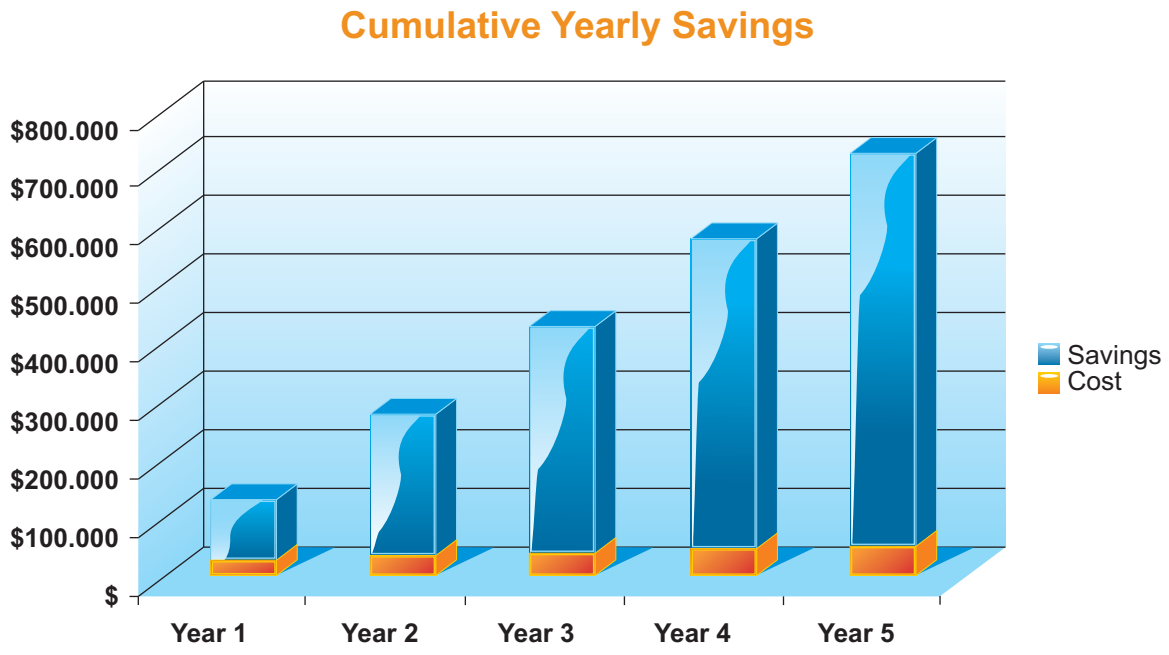
Enhances Portability
Our RoboForm2Go version runs from a USB Flash Drive so employees can take passwords, contacts and bookmarks with them.

RoboForm Enterprise Solves The Most Common and Costly Password Management Challenges

The Problem	RoboForm Enterprise Solution
▪ Employees forget their passwords and call the IT helpdesk, wasting time and money.	▪ RoboForm requires employees remember ONE secure master password. RoboForm remembers the rest of your employees' passwords.
▪ Employees write down their passwords on notepads, stickies or store them in insecure computer files.	▪ Since RoboForm remembers all your employees' passwords, there is no need to write them down. In addition, all RoboForm files are secured using strict AES (256 Bit) encryption.
▪ Employees use simple, easy to remember, but also easy to guess passwords.	▪ Employees can easily remember the one strong password needed to access RoboForm. RoboForm remembers the rest, so your employees' can now use strong passwords.
▪ Employees' computers may be infected with Keyloggers.	▪ RoboForm's master password can be entered using a virtual keyboard. RoboForm bypasses the keyboard entirely with its automated login technology.
▪ Employees may share their passwords.	▪ With RoboForm's dual password function, an employee is free to share a Passcard with another employee without the second employee ever knowing the actual username and password combination for the Passcard. This feature is great for providing temporary access to someone without having to change or share the underlying password!

Immediate Return on Investment

Poor or incomplete password management can seriously impact the safety and security of your organization. It can also have a major impact on IT costs. According to most estimates, around 40 percent of all calls to helpdesks are password-related, and most of these calls involve requests to retrieve or reset forgotten passwords. With each call costing around $30, password self-service translates directly into significant cost savings and immediate relief for your helpdesk staff.



This chart shows the annual savings and return on investment for a company with 1,000 employees and a conservative 70 percent of those employees using RoboForm Enterprise.

RoboForm Enterprise is a Better, Easier, and More Cost-effective Solution than Multi-factor Authentication or Enterprise Single Sign-On

	RoboForm Enterprise	Multi-factor Authentication	Enterprise Single Sign-On
No Additional Hardware	☑	☒	☑
Integrates with Existing Architecture - No mass Integration Required	☑	☒	☒
Easy Deployment to All Employees	☑	☒	☒
Low-risk entry can be tested before mass deployment	☑	☒	☒
Defeats Phishing and Keylogging	☑	☒	☒
Immediate ROI	☑	☒	☒
Client-based, distributed solution	☑	☒	☒

Conclusion

An effective enterprise password management approach increases security without decreasing productivity or increasing costs.

It's essential to create a solution that your employees will actually follow and use. The solution should store passwords more securely, encourage employees to adhere to stricter password practices, and allow employees to remember a reduced number of passwords.

RoboForm Enterprise is a unique solution that allows your organization to use stronger password management practices without compromising security or increasing costs. The deployment is easy, takes minutes instead of months, and can be fully tested prior to deployment. We've taken away all the risks.

To learn more about RoboForm, contact Scott Vanatter at (703) 218-1851 x118, or svanatter@siber.com.

About Siber Systems

Our mission is create world class innovative software products designed to make using a computer easier, faster, and more secure for individuals and enterprises around the world. Siber Systems is a privately-held company, incorporated in 1995 in the Commonwealth of Virginia, with offices in Germany, Japan, and Russia.

Siber Systems was originally founded to create useful commercial technologies from scientific findings in the area of text parsing, compilation and transformation. Our CobolTransformer was released in 1997 and is licensed by Fortune 500 companies such as IBM, Computer Associates and Fujitsu Software. Our Cobol Data Viewer, a premier product used to recover data from Cobol data files, was released in 1998 and is licensed by hundreds of companies and continues to be actively licensed today.

We released RoboForm, our first consumer product, in 1999. Since then RoboForm has been translated into over 30 different languages and has millions of active users worldwide.

In 2004 Siber Systems developed RoboForm2Go, one of the first applications designed to run natively from USB flash drives. RoboForm2Go, a portable version of RoboForm, allows users to take their passwords with them. Simply plug a USB flash drive into any computer, anywhere in the world, and enjoy all the conveniences of RoboForm.

Our latest product, GoodSync, is an easy and reliable file synchronization program that was released in 2006 and already enjoys favorable reviews from IT users and the press. Our software has an outstanding reputation and has received hundreds of media reviews, including reviews by the Wall Street Journal, New York Times, Morningstar, Barron's, Financial Times and others. Our software was named PC Magazine Editor's Choice and CNET's Best Software of the Year.

Contact Information

If you would like to learn more, schedule a demo, or download a free trial version, we encourage you to contact Scott Vanatter, VP of Enterprise Sales at (703) 218-1851 x 118, or at svanatter@siber.com.

World Headquarters Address

Siber Systems, Inc.
11781 Lee Jackson Memorial Highway, Suite 260
Fairfax, VA 22033

+1-877-ROBOFORM (762-6367)
+1-703-218-1851

www.roboform.com/enterprise