

**SiberSystems**

**white paper**

# **Solving the Password Management Paradox**

**Defining the Problem and Reviewing the Four Best-Known Solutions**

## Table of Contents

<b>Executive Summary</b> .....	2
<b>I. The Challenge of Password Security</b>	
- Need for Security .....	3
- Protecting Your Data .....	3
- Basics of Authentication .....	4
- Problems with Passwords .....	4
- The Paradox of Password Policies .....	6
- Cost of Help Desk Calls .....	6
- User Support Itself Creates Security Problems .....	7
- State of the Problem .....	7
<b>II. Solutions</b>	
- A Strong Password Policy .....	8
- Password Synchronization .....	9
- Single Sign-On .....	10
- Single Sign-On Alternatives (Enterprise Password Management) .....	11
<b>III. The Ideal Solution</b>	
- Increases Security .....	12
- Reduces Employees' Passwords .....	12
- Improves Employee Productivity .....	12
- Easily Integrates Into Existing Systems .....	12
- Reduces Help Desk Costs .....	12
- Provides an Immediate Return on Investment .....	12
- Provides a Sustainable Solution .....	12
- Offers a Trial .....	12
<b>IV. The RoboForm Enterprise Solution — Key Features and Benefits</b>	
- Increases Security While Reducing Employees' Passwords .....	13
- Improves Employee Productivity .....	13
- Easily Integrates Into Existing Systems .....	14
- Reduces Help Desk Costs .....	14
- Provides an Immediate Return on Investment .....	14
- Provides a Sustainable Solution .....	14
- Trial Version Available .....	14
<b>V. How Do I Start?</b> .....	15
<b>About Siber Systems</b> .....	16
<b>Appendix — Three Password Management Techniques</b> .....	17
<b>References</b> .....	18

## Executive Summary

Organizations need to protect their data and restrict access to enterprise resources to authorized users.

Many companies attempt to address their security concerns by simply implementing stronger password policies, requiring employees to remember more and stronger passwords for all applications.

However, most employees can not remember more than one or two strong passwords, so they won't follow the policy, resulting in *less* network security and *more* requests to the help desk to reset lost passwords. This is what we refer to as the Password Management Paradox — the assertion that requiring too many strong passwords will actually *decrease* overall corporate security.

A company has several options available to protect access to sensitive data, including...

- **A Strong Password Policy**
- **Password Synchronization**
- **Single Sign-On**
- **Single Sign-On Alternatives (Enterprise Password Management)**

Effective security requires a policy that users will actually follow and that doesn't tie up the IT help desk.

This paper reviews the challenge of password management and security, discusses the paradox of strong password policies, evaluates several possible solutions, and recommends a password management solution that is cost effective and easy to implement.

## The Challenge of Password Security

### *Need For Security*

One of the first things a new employee receives is a password to access his computer, the company network, and whatever applications or services he needs to do his job. The logic behind the password is simple. The company wants to limit access to authorized personnel.

If that's the real goal, you have to wonder why a company requires passwords when you can be pretty sure the employee will...

- **Forget it, using up their time and the IT staff's valuable time to reset the password,**
- **Write it down where other people can get to it,**
- **Share it with other employees, or**
- **Use a simple password that anyone can guess.**

Access to your network and information is a crucial part of your business that needs to be protected, but passwords alone aren't always the best solution.

### *Protecting Your Data*

Information is one of a company's strategic resources. The company owns valuable proprietary processes, sensitive customer information, private vendor lists, and strategic goals that have great value – and may be attractive targets for competitors or thieves. In some cases companies have a legal obligation to protect that data. Data also has to be protected from accidental (or intentional) corruption, and IT professionals must ensure that company data is accessible or deliverable when necessary.

As a result, companies spend a significant portion of their IT budget on managing and protecting information. Sometimes business interests collide. More security sometimes means less productivity, more cost and less return on business investment.

A company's data can be lost or stolen if network users don't follow basic security procedures. Lost data can mean...

- **Lost time**
- **Lost money**
- **Lost opportunities**
- **A lost competitive edge**
- **A crippling legal liability and a serious public relations problem, if the company loses customer or client data**

### **The Real Cost of Poor Password Security**

"Just one naive user with an easy-to-guess password increases an organization's risk."<sup>1</sup>

"The average cost of a data breach rose to more than \$6.3 million last year"<sup>2</sup>

A CERT survey of IT professionals found that e-crimes are on the rise.

- **49 percent of respondents reported experiencing an e-crime in 2006, vs. 38 percent the previous year.**
- **33 percent reported an increase in the number of "security events."**
- **The survey reported that the average annual monetary loss from e-crime is almost half a million dollars.**
- **26 percent of respondents directly attributed password management policies to the deterrence of a potential criminal.**<sup>3</sup>

Financial companies have faced heavy fines for lost laptop computers. A password breach is at least as serious, because it may give an intruder access to network assets as well as those on a local machine.<sup>4</sup>

## The Challenge of Password Security

### *Basics of Authentication*

Securing your data means making sure only the right people have access to it, which requires authentication, in which a potential user has to present something...

- **That he knows (a password or PIN)**
- **That he has (a token, such as a smart card)**
- **That he is (a voice print, fingerprint or retina scan)**

Biometrics is the strongest form of authentication, but it is also the most expensive, and out of the range of most companies. Tokens are very effective, but are also very expensive to implement in an enterprise environment due to the cost of integrating a token-based system with network resources. As a result, passwords are the best solution for most operations.

### *Problems with Passwords*

A password-based security system is the best option for most companies, but such systems do have their problems.

Passwords are a burden on users, who view them as an obstacle to getting the information and services they need in a timely fashion. Having to enter different usernames and passwords several times a day - and especially repeated erroneous attempts - interrupts an employee's usual work flow, often at the most inopportune times.

Network administrators, on the other hand, are keenly aware of the need to limit application and network access to authorized personnel and therefore prefer strict password policies. This inherent conflict of interest can result in a battle of wills between those charged with protecting data and those charged with using that data.

In a recent survey of over 600 U.S. IT professionals, Siber Systems uncovered some surprising statistics on password use and abuse.

- **Too many passwords.** Over half of all respondents said the average employee in their firm is required to remember three to five passwords, with an additional 26 percent saying the number ranges from six to ten or more; 16 percent of "power users" reported having over 100 passwords.
- **Passwords required too often.** 49 percent responded that employees are required to use passwords more than 25 times per week, with 8 percent stating the number of password uses exceed 100 per week.
- **Unprotected passwords.** 66 percent stated that employees write down or store passwords in unsafe places, creating a security problem for their companies.

### **Employees Take Short-Cuts with their Passwords, Compromising Security**

"Two temporary data entry clerks and one permanent employee were able to embezzle almost \$70,000 from their company by fraudulently using other employees' computer accounts. The employees within their group openly shared their passwords to enhance productivity." <sup>5</sup>

## The Challenge of Password Security

### The Insider Threat

Most insiders seeking to do harm don't use their own username and password to gain access to company resources. They either compromise an account or use another employee's account or a shared account.

"Computer account and password management policies and practices are critical to impede an insider's ability to use the organization's systems for illicit purposes."<sup>5</sup>

Other studies have shown that the password burden can be far worse. In one study, over a quarter of all respondents had to manage over 13 passwords.<sup>6</sup>

Inevitably, employees need passwords for systems or applications that they access only infrequently, which makes it harder for them to remember the password.

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 policies.

Power users and even rank and file knowledge workers simply have 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 an increasing amount of 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.

All the while, employees are...

- **Writing down passwords on sticky notes and putting them on computer monitors**
- **Sharing passwords with co-workers, making it impossible to track who has access to what**
- **Using simple passwords that can be guessed**
- **Falling for phishing schemes, where they're tricked into providing a password to the wrong application or website.**
- **Storing their passwords in their web browser.**

Even with good password policies, passwords may be transmitted over a network in plaintext, or in a format that is easily converted to plaintext. Often enterprise passwords are stored in an insecure location or in insecure backup media.

## The Challenge of Password Security

### The Paradox of Password Policies

When developing a password policy, it's important to consider the paradox of password security. A weak policy is inherently insecure, but an overly stringent policy will result in users breaking the rules – by writing down or sharing passwords or storing them in an unprotected computer file.

It's a good idea to encourage users to change their passwords on a regular basis because if an attacker gets a hashed or encrypted copy of a password, the hacker can eventually break the password. Changing passwords on a regular basis can help mitigate that risk.

However, requiring users to change their passwords invites even more user fatigue, creating more passwords to remember, which invites breaking the rules, and causes more helpdesk calls to reset lost passwords.

Ideally a company could require employees to remember and properly use many secure passwords resulting in optimal security. In reality, after a certain point, as the number and strength of required passwords *increase*, security begins to *decrease* as employees take short cuts with their passwords. **Requiring too many strong passwords actually has an inverse effect on corporate security**, as indicated in the figure below.

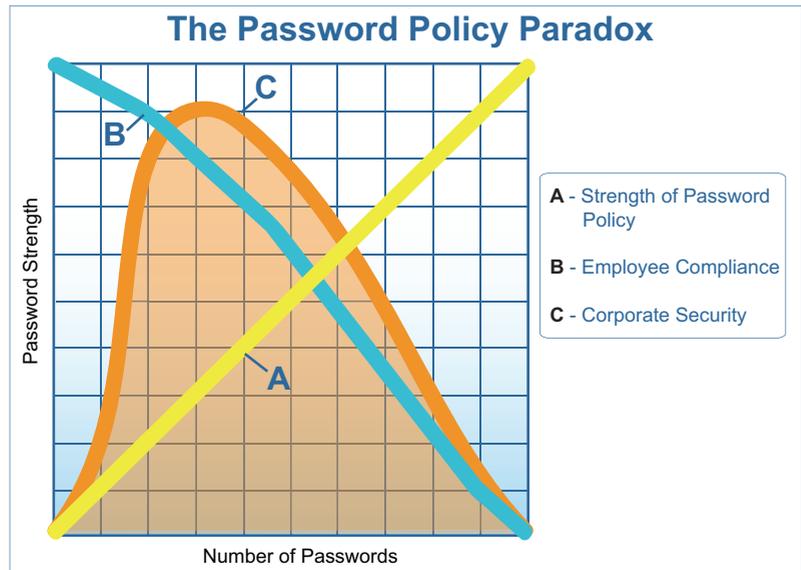
#### Password Management Savings

"Implementing an Identity Management solution immediately reduces the number of passwords required by each customer to access the resources they need to perform their duties."<sup>7</sup>

The average cost of resetting a single password in a medium-sized organization is about \$20 per request. This figure can be reduced to around \$3 by automating portions of the reset process with an Identity Management system.<sup>7</sup>

The volume of help desk calls can be reduced by 30 percent by implementing an Identity Management system.<sup>7</sup>

45 percent of help desk calls are for password resets. Automating password resets reduces this call volume by approximately one-third."<sup>8</sup>



### Cost of Help Desk Calls

Industry reports on help desk costs show that 20 to 40 percent of these calls involve resetting lost passwords,<sup>9</sup> that each reset takes between six and 15 minutes, and that each help desk call costs between \$25 and \$50.<sup>6</sup>

The number of help desk requests an organization receives will vary according to the strength of the organization's password policy. Some studies show that an average user can request 10 password resets per year.<sup>7</sup>

The cost of the inevitable increase in help desk calls must be factored into the cost of a password policy.

## The Challenge of Password Security

### *User Support Itself Creates Security Problems*

As has been mentioned, one consequence of a strong password policy is an increase in calls to the help desk. But that's a bit of a catch-22, because user support can itself create security problems.

An intruder may pose as an employee and get the help desk to reset a password for the intruder. This threat requires the help desk to authenticate the user, which raises a whole new level of security issues – i.e., ensuring that the means by which users authenticate with the support staff is itself secure.

When the support staff resets a user's password, the support staff often knows the new password, which isn't always a good idea. Depending on the system, the wrong people might have access to the password reset function.

### *State of the Problem*

Many companies report that "password inflation" – the growth of the number of passwords used and the frequency of their use – negatively impacts productivity as well as security. While 79 percent of those taking the Siber Systems survey report that security is their number one password management concern, 39 percent also reported "Lost Employee Productivity or Frustration" as an issue. Siber predicts that this percentage would increase if the company interviewed business unit managers, in charge of operations. The survey consisted mostly of IT executives, who, naturally, are more concerned with security. In addition, 31 percent said that help desk hours are either lost or spent in frustration by support personnel.

Companies need a way to increase security while decreasing help desk calls and expense. A strict password policy alone won't do it, since users won't follow a strict policy for more than a couple passwords. Companies need a solution that controls access to resources with a strong password policy without reducing productivity or increasing IT help desk calls.

## Solutions

Many companies have researched and invested in a lot of different options to solve the need for security without burdening the worker with oppressive requirements. The most common strategies are discussed below, including a review of their strengths and weaknesses.

- **A Strong Password Policy**
- **Password Synchronization**
- **Single Sign-On**
- **Single Sign-On Alternatives (Enterprise Password Management)**

### *A Strong Password Policy*

The first, and from one point of view, the simplest option for increased security is to implement a strong password policy. In the ideal world a company would establish a strong password policy, employees would follow that policy, corporate data would be secure and help desk costs would be minimal.

The single most important thing for a user to remember when creating a new password is to make the password hard to guess, but easy to remember. That's easier said than done, but some tried and true guidelines can help users create passwords that are more secure than what they're currently using.

A good password is first, a combination of letters, numbers, and symbols that cannot be found in a dictionary. A password should be at least six characters long and should not have any personal information such as the user's name, child's name, occupation, telephone number, address or birth date. A combination of letters, numbers and symbols will work best, although some systems allow a different set of characters than others, so the use of characters like the semi-colon can be problematic. It's also important to use a mixture of capital and lower-case letters to make a password even more difficult to guess.

Users should change their passwords regularly – once every three months at a minimum.

Companies can train their employees to use several techniques that can make existing passwords more difficult for hackers to crack. The method chosen should be easy and understandable to make stronger passwords without much effort. Three simple, yet effective techniques are discussed in the Appendix.

The main benefit of implementing a strong password policy is that it avoids the start-up and implementation cost of some of the other solutions. But as discussed above, it may increase help desk costs and user frustration and result in lost productivity.

To implement a strong password policy, a company must research techniques, establish a policy, train its employees, and adjust their authentication processes or systems to reflect the harder password requirements.

There are many potential downsides. Many studies show that employees can't or refuse to remember multiple passwords, and take shortcuts – as discussed above – which creates a less secure environment.

#### **A Strong Password Policy: Summary Benefits and Drawbacks**

##### *Benefits*

- Little or no new software is required
- Required training is fairly minimal and inexpensive

##### *Drawbacks*

- Employees are unlikely to comply with the policy
- It may result in increased help desk costs and lower productivity

## Solutions

### *Password Synchronization*

Password Synchronization allows users to have a single password, subject to one security policy, that grants access to multiple machines, systems or devices. It can be used, for example, to synchronize passwords between Windows and Unix systems.

A password synchronization system is easier on the user, who only has to remember one password. This creates a more secure environment because users are able to remember one strong password and are less likely to share it or write it down.

Password Synchronization is sometimes said to be easier than single sign-on because there is no client software to deploy. However, password synchronization creates implementation costs for the IT department, and raises some security concerns.

IT must develop a password policy that will work for each application, and each application has to be configured to work with the synchronizing system. This can be a major expense of time and resources.

The entire system can only be as secure as the least secure application. For example, if one application only allows a 6-character password, limits the password to letters and numbers and is not case specific, all the applications will be similarly limited. Therefore, very insecure systems should not be included in a password synchronization scheme, which tends to defeat the purpose of synchronizing passwords.

In order to synchronize passwords in an enterprise environment, the passwords must be stored and/or transmitted across the network. This process itself must be secured.

Password Synchronization can be an effective tool, but its effectiveness will depend on the nature of the applications being synchronized and their internal security rules.

#### **Password Synchronization Summary Benefits and Drawbacks**

##### *Benefits*

- Can limit the number of passwords users have to remember
- Since users have to remember fewer passwords, they are more likely to comply with a strong password requirement

##### *Drawbacks*

- Synchronizing multiple applications can be expensive and time-consuming
- The system is only as secure as the most insecure application

## Solutions

### Single Sign-On

Single Sign-On (SSO) is an authentication method that provides end users with the ability to login one time, gaining authenticated access to all their applications and resources. SSO is an additional layer that sits on top of all applications and web resources. A user logs in to this system, which then takes care of all logins to enterprise assets.

The advantage of SSO, like password synchronization, is that users only have to remember one strong password. A single sign-on can also help establish an audit trail – i.e., a means to track which users were using which applications – and makes it easier to identify orphaned (unused) user accounts.

In order to implement SSO, the IT department must gather the passwords and login methods for all enterprise resources, store those passwords in the SSO system, and configure the system to implement all the login methods for each resource. This centralized database of passwords is a major security risk, because the entire enterprise will be compromised if an unauthorized user gets access to the database.

In other words, Single Sign-On has a built-in disadvantage, because access to the SSO system is essentially the “keys of the kingdom.”

SSO also presents a challenge with regard to partner sites and resources, since IT does not always have the ability to configure the SSO system to work with third-party systems.

Resetting all the passwords in an SSO environment can also be very costly since the passwords have to be reset across a range of applications with different security rules.

Given the nature of the systems integration, implementing an SSO system takes a tremendous amount of time and resources and is very costly. In recent months many companies have paused or completely stopped their SSO implementations in search of alternative solutions.

#### Single Sign-On Summary Benefits and Drawbacks

##### Benefits

- Users only need one password to access all system resources
- Since users have to remember one password, they are more likely to comply with a strong password requirement

##### Drawbacks

- SSO can be very expensive and time-consuming to implement
- SSO is hard to implement with partner sites
- The single repository of passwords provides the “keys to the kingdom” for a hacker

#### Single Point of Failure

“When you reduce authentication to a single point, a breach at that single point also compromises every application a user is authorized to access. In other words, when an employee, authenticated on the network, leaves the office to go to lunch, and neglects to lock down his or her computer, everyone with physical access to that computer immediately—and transparently—has access not only to the applications left open on the desktop, but to every application to which that user has access.”<sup>10</sup>

## Solutions

### Single Sign-On Alternatives (Enterprise Password Management)

In the past few years some companies have developed enterprise password management solutions that have the same advantages of SSO and Password Synchronization, but without many of the known disadvantages such as cost, integration effort, and a single password source.

Enterprise password management is a client-based software solution – meaning that software is installed on the employees' laptops and desktops. The software requires the use of one password, a master password, but then remembers the employees' other passwords and logs them into corporate websites and systems automatically.

Since it's a distributed software solution, the passwords reside on each employee's computer, rather than in one central repository. The passwords are securely stored with strong encryption with the master password as the encryption key. Having passwords securely distributed significantly reduces the threat of a major security breach.

The software is designed to work with a company's existing systems. A large integration effort is not required, which keeps costs significantly lower than SSO and Password Synchronization solutions.

Some systems come with policy editors that allow IT staff to completely customize the solution to their exact security standards. The policy editors are easy to use, typically consisting of a checkbox of options to turn on and off. The application can usually be customized in less than an hour.

Currently, the main disadvantage of enterprise password management solutions is that they tend to work only with Windows-based systems. Therefore the software may have some difficulty integrating with some very old legacy systems, a problem commonly identified with SSO solutions as well.

#### Alternative Single Sign-On (Enterprise Password Management) Summary Benefits and Drawbacks

##### Benefits

- Users only need one password to access all system resources
- Since users have to remember one password, they are more likely to comply with a strong password requirement
- Alternative SSO is less expensive and less time-consuming to implement than SSO and Password Synchronization
- There is no single repository of passwords.

##### Drawbacks

- The technology is younger than SSO and Password Synchronization
- Some companies may not favor client-based/distributed solutions

#### Effective Identity Management Reduces IT Costs

Studies show that the time spent setting up a new user can be up to 29 hours, but that implementation of an Identity Management System can reduce that time up to 75 percent.<sup>7</sup>

## The Ideal Solution

As discussed above there are many different password management options for companies to consider. Each solution has its own strengths and weaknesses. The ideal solution meets the following tests.

**Increases Security** – The main reason a company wants to implement a password management solution is to increase the security surrounding corporate data and assets.

**Reduces Employee Passwords** – Many studies show that employees can only remember one or two secure passwords, and when they are required to remember and use more than one or two passwords they begin to take short-cuts. These short-cuts have an adverse effect on corporate security.

**Improves Employee Productivity** – Salaries are rising, employee workloads are increasing, and in general, demands are higher. The less time an employee spends worrying about passwords or calling the helpdesk for password resets the more time the employee will spend doing the work of the company.

**Easily Integrates Into Existing Systems** – The sooner the solution is implemented, the sooner a company can enjoy the benefits of increased security and employee productivity. IT staff are over-burdened already, so taking on an additional project that requires a large amount of time and attention leaves less time to focus on other priorities and initiatives.

**Reduces Help Desk Costs** – If a solution results in increased help desk costs, then all a company has effectively achieved is to shift the expense of employee password management from one budget line to another. A good solution will also reduce the burden on the IT help desk staff.

**Provides an Immediate Return on Investment** – IT budgets are stretched and companies face increased scrutiny to provide better and quicker returns on investment. The more a company invests in a password management solution, the longer it takes for the company to realize a return. The most expensive solutions are often not the best solutions.

**Provides a Sustainable Solution** – After a quick and easy implementation, the chosen solution should afford end users and IT managers an easy way to maintain password changes. The solution should easily work with whatever kind of logon is presented to the end user.

**Offers a Trial** – It's much easier to make a buying decision when you can try the solution before you buy it. Ideally a company can roll out the trial solution to several employees and solicit feedback before making an investment. A worst case scenario is to invest in a very expensive solution, go through months, if not years of integration, only to find out that the solution was not what was promised and does not solve the problems the company initially set out to resolve.

## The RoboForm Enterprise Solution - Features and Benefits

RoboForm Enterprise is an advanced, full-featured Password Management Solution that employees will actually appreciate and enjoy using. The solution provides a client-based alternative solution to Enterprise Single Sign-On (SSO).

### *Increases Security While Reducing Employees' Passwords*

**One Master Password** – End users will only be asked to remember one strong Master Password. RoboForm will then use strong encrypted passwords to provide access to web sites and applications.

**Strong Password Policies Followed** – Using software to reduce employee's passwords means end users will be empowered to actually follow strict company security and password standards, improving overall IT security and protecting sensitive corporate data.

**Protects Your Passwords to Secure Your Network** – Access to RoboForm is controlled by a single strong password. Once the user logs in to RoboForm, the software securely stores usernames, passwords and other confidential information on the user's computer using powerful AES encryption. When a user visits a password-protected website or starts an application, RoboForm automatically retrieves authentication data and logs the user in with one click.

**Safeguards Users From Identity Theft** – A RoboForm user doesn't have to worry about remembering passwords on multiple systems, so the user can pick a very strong password. RoboForm will remember it and enter it when the user tries to access that resource. Since a RoboForm user doesn't have to key any authentication data, and since it only provides authentication data to valid websites, it protects users against keylogging and phishing scams.

**Dual Master Password Increases Protection from Employees** – The Dual Master Password feature enhances security options by allowing users to login to certain sites without the user ever having access to the actual password for that site.

**Strong Encryption Mitigates Security Risks** – In a standard SSO implementation all passwords are stored in a central database, so if anyone gets access to the database, the entire Enterprise will be compromised. Resetting all these passwords is a dubious and costly effort. With RoboForm, the password files are encrypted using AES with a Master Password as a key. Each employee Master Password is known only to the employee, and stolen Passcard files remain unusable to an outsider who does not know the Master Password.

### *Improves Employee Productivity*

**No More Forgotten Passwords and Countless Password Resets** – End users, especially power users, will enjoy a productive workflow and will not have to try over and over again to remember forgotten usernames or passwords. Minutes lost, especially when on a deadline, can be very costly in hard dollars, but also in a productive and creative work product.

**Users Enjoy One-Click Logins** – RoboForm's powerful form-filling technology allows users to login to websites automatically. The user simply selects a RoboForm Passcard and the system takes over, navigating to the website, entering the correct username and password and clicking the submit button. RoboForm also manages online checkout, registration and other forms.

## The RoboForm Enterprise Solution - Features and Benefits

### *Easily Integrates Into Existing Systems*

**Same Day Solution** – Rather than taking weeks, or months – or years to implement, RoboForm Enterprise can be deployed in a day, even within an hour.

**No Implementation Phase** – Unlike single sign-on, RoboForm doesn't require the IT department to collect all the authentication information for all the applications and websites users will access. Rather, when a user goes to a new site or tries to use a new application and enters a password, RoboForm securely stores that password so the next time the user tries to access that resource, RoboForm will automatically provide the authentication data. The user doesn't have to remember the password, and it's so intuitive that employees learn to use it by simply using it.

**Intuitive Interface Means Less Work For Support** – RoboForm makes user interaction a breeze, so a user can start using RoboForm without training. With its intuitive interface and online help, employees easily understand how to use RoboForm's main features, and since a server component is not required, support costs will be close to zero.

**Policies Allow System Administrators to Customize Everything** – RoboForm Policies are a set of rules and options that a System Administrator can force onto all RoboForm users. Using these policies, System Administrators can customize all aspects of RoboForm behavior. For example, administrators can set the minimum length of the Master Password, set the minimum number of digits in a password, control the use of upper and lower case characters, etc.

### *Reduces Help Desk Costs*

**No More Help Desk Password Resets** – End users have no need to contact the Help Desk, as RoboForm Enterprise automatically remembers their usernames and passwords and automatically provides their login credentials as they go about their usual activities.

### *Provides an Immediate Return on Investment*

**Less Than Two Months** – RoboForm provides an immediate return on investment through increased employee productivity and reduced helpdesk calls. Most companies see a positive return on investment in as little as two months.

### *Provides a Sustainable Solution*

**Automatic Password Management** – RoboForm learns on-the-go with no additional programming. When end users change passwords, RoboForm Enterprise automatically remembers the new password as it is entered. As new resources are made available to end users, RoboForm Enterprise automatically remembers logon information in the end users' normal work flow.

### *Trial Version Available*

Most solutions require customers to make a blind-faith investment based on a sales pitch. Siber Systems encourages companies to use the trial version for 30 days. The trial version is the actual all-inclusive product, not a slim-downed version with the promise of full features after purchase. RoboForm allows companies to fully test the software to be confident it meets their goals and objectives.

## How Do I Start?

We hope this white paper has given you a thorough understanding of your password management options. We're so sure RoboForm will meet all your password management needs that we will let you try it for 30 days.

Visit our website - [www.roboform.com/enterprise](http://www.roboform.com/enterprise) - to download a 30-day trial of the full RoboForm Enterprise product, or for additional information such as an executive summary, product fact sheet, or other white papers, including a password management survey of top IT executives.

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](mailto:svanatter@siber.com).

### ***World Headquarters Address***

Siber Systems, Inc.  
11781 Lee Jackson Memorial Highway, Suite 260  
Fairfax, VA 22033  
+1-877-ROBOFORM (762-6367)

[www.RoboForm.com/Enterprise](http://www.RoboForm.com/Enterprise)

## About Siber Systems

### Siber Systems' Products

- RoboForm
- RoboForm2Go
- RoboForm Enterprise
- GoodSync
- GoodSync Enterprise
- Cobol Data Viewer

Our mission is to 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. Our company headquarters is located in Fairfax, Virginia, just outside the Washington, D.C. beltway. We also have 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, CA 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.

After years of working directly with companies to deliver customized enterprise solutions, in 2007 we added a Policy Editor, more deployment and activation options, as well as additional features to create our RoboForm Enterprise product.

Our latest product, GoodSync, is an easy and reliable file synchronization program that already enjoys favorable reviews from consumers, enterprises, 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, CNET's Best Software of the Year and PC World's 25 Products We Can't Live Without.

## Appendix – Three Password Management Techniques

Companies looking to implement strong password policies that their employees will follow should train their employees on different techniques.

The goal of any strong password policy is to make existing passwords more difficult for hackers to crack, yet simple enough for employees to remember and use. There are several techniques employees can use to generate strong passwords that are easy to remember.

Three simple, yet effective techniques are discussed below.

### Form an Expression

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

### Substitute Numbers for Letters

Choose a word as a password, but substitute similar looking numbers for letters. 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	S...5
I...1	G...6
Z...2	L...7
E...3	B...8
H...4	

It's not necessary to associate every number with a letter. It is important to remember the list of associated letters and numbers.

### Keyboard Mapping

Choose a password and then translate it with a keyboard mapping system. For example, an “upper-left” keystroke system would pick the letter to the upper-left of the actual key. Using this method, “Gandalf” would become Tqheqor. “Football” would become r995gqoo. This method is hard to use at first, but muscle memory quickly takes over and the password will be easy to enter. But if it is forgotten, the pattern is simple enough, which makes it easier for the user to reconstruct the password.

## References

- 1 – Pethia, Richard D., September 1999, Testimony to the Commerce and Economic Development Subcommittee on Electronic Commerce ([http://www.cert.org/congressional\\_testimony/PA\\_ecommerce\\_hearing\\_sep99.html](http://www.cert.org/congressional_testimony/PA_ecommerce_hearing_sep99.html))
- 2 – “The No Tech Hacker,” Forbes, Feb. 2008  
[http://www.forbes.com/2008/02/28/long-hacker-csc-tech-security-cx\\_ag\\_0229hacker.html](http://www.forbes.com/2008/02/28/long-hacker-csc-tech-security-cx_ag_0229hacker.html)
- 3 – 2007 E-Crime Watch survey sponsored by CSO Magazine, the U.S. Secret Service, CERT Program, and Microsoft Corp.
- 4 – “The true cost to a business of a lost laptop.” <http://www.creativematch.co.uk/viewnews/?93510>
- 5 – Common Sense Guide to Prevention and Detection of Insider Threats 2nd Edition – July 2006, Carnegie Mellon University CyLab
- 6 – “RSA Security Survey Reveals Multiple Passwords Creating Security Risks and End User Frustration”  
[http://www.rsa.com/press\\_release.aspx?id=6095](http://www.rsa.com/press_release.aspx?id=6095)
- 7 – Gordon, T., “Quantifiable Benefits of Implementing Identity Management Systems,” University of Salford, Information Services Division, 2005.
- 8 – Quoted from PricewaterhouseCoopers/Meta Group Survey 2002, titled “META Group White Paper: The Value of Identity Management” in Password Management, Chapter 1: Introduction to the Password Management Paper  
<http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2pass.mspx>
- 9 – Studies indicate a range from 20 to 50 percent, as follows:
  - 20 percent  
Cox Installs Password Software to Ease Help-Desk Burden, <http://www.itjungle.com/mso/mso120203-story01.html>
  - 30 percent  
Use Strong Authentication Software to Reduce Password Support Costs, [http://www.biopassword.com/library/BP\\_ROI.pdf](http://www.biopassword.com/library/BP_ROI.pdf)
  - 40 percent  
Self Password Reset,  
<http://manageengine.adventnet.com/products/self-service-password/self-service-password-reset.html>  
Single Sign-On, [http://www.encentuate.com/library/pdfs/encentuate\\_datasheet\\_esso.pdf](http://www.encentuate.com/library/pdfs/encentuate_datasheet_esso.pdf)
  - 30 to 50 percent  
Password Self-Service: Taking the Strain Off of Help Desks,  
[http://www.novell.com/solutions/securityandidentity/passwordtour/password\\_self-service.pdf](http://www.novell.com/solutions/securityandidentity/passwordtour/password_self-service.pdf)
- 10 – Single Sign-On: The High Cost of Convenience, <http://www.devx.com/opinion/Article/21476>