

Are passwords really free?

A closer look at the hidden costs of password security

Driven by many factors—including consumer demand for enhanced security, compliance pressures and a desire to re-energize the growth of e-business—leading enterprises are making strong authentication a core component of their e-business strategies. Unlike password management systems, strong authentication delivers the security needed to safely conduct business online. But these enterprises are also discovering an unexpected benefit: dramatically lowered operating costs. That's because the hidden costs associated with the deployment and ongoing management of "free" password security actually outweigh the perceived high price tag of implementing strong authentication. Coupling this with the new business opportunities that come with enhanced security—new revenue streams and process efficiencies—makes for a compelling ROI. In this paper, RSA Security explores the total cost of ownership (TCO) associated with password security, helping enterprises to make an informed decision when contemplating their strategic move toward stronger security.

TABLE OF CONTENTS

I. INTRODUCTION	1
II. TOTAL COST OF OWNERSHIP	1
Acquisition Cost	1
Deployment Costs	1
III. MANAGEMENT COSTS	2
Total Cost of Ownership - Summary	3
IV. SECURITY EFFECTS	3
THE BOTTOM LINE	
Relative Security	3
Passwords as a "Security" Mechanism	4
Are these concerns real? The answer is yes!	4
Strong Authentication for Enhanced Security	4
V THE ROI BENEFITS OF STRONG AUTHENTICATION	5
Increased Revenue	5
Lower Costs	5
Compliance	6
Mitigated Risk	6
CONCLUSION	6
ABOUT RSA SECURITY	6
APPENDIX A — 3-YEAR TOTAL COST OF OWNERSHIP WORKSHEET	7
APPENDIX B — ESTIMATING RISK	8

INTRODUCTION

As more and more business processes move online, many enterprises are evaluating stronger security than that provided by traditional passwords. However, the decision to replace embedded password security solutions with stronger authentication is a complicated one, involving many factors. One must consider the appropriateness of user fit (usability, portability and multi-purpose functionality) and the appropriateness of corporate fit (strength of security, interoperability and integration, scalability and future flexibility). As with any significant technology investment, cost is always a consideration. (Please see the [Authentication Scorecard](#) to learn more.)

TOTAL COST OF OWNERSHIP

When considering any user authentication technology—ranging from passwords, tokens, digital certificates to biometrics—to accurately understand the true cost of ownership it is necessary to look beyond the acquisition costs and consider the on-going expenses associated with deploying and managing the solution. For the purpose of this paper we will develop a spreadsheet to help calculate the acquisition, deployment and management costs of passwords, considering a three-year period for a 1,000 user environment.

Acquisition Cost

Password management systems have a major advantage over all other authentication technology in that they are generally available “free of charge” and are embedded or otherwise provided for within operating systems, communication devices and business applications. Further, they do not require the purchase of any special devices or software for the end users.

Strong authentication technology, on the other hand, requires the purchase of a server software license and RSA SecurID tokens for each end user. Annual maintenance for the software license is also highly recommended.

Remember, however, that acquisition cost is only one of three factors that determine the total cost of ownership. The others are the cost of deployment and the cost of ongoing management.

Deployment Costs

Deployment costs will vary widely between different user authentication technologies. To formulate an estimate of these costs, it is first necessary to assign a dollar value to a knowledge worker’s time in order to calculate the impact each solution will have on deployment costs. For the purpose of this exercise, we will assume a knowledge worker’s fully burdened cost to a company to be \$40 per hour or approximately \$80,000 per year. This assumption may not be accurate for your particular situation and you should adjust any calculations accordingly.

The first password-related expense that most companies will incur is associated with establishing a user account. If the information that will be protected is valuable, a company will want to establish a process and a policy for approving a user’s request for a password. A user fills out and submits a request form, a manager reviews and approves the request and someone in the IT department establishes an account for the user. This one-time user initiation process typically takes a total of 15 to 20 minutes of personnel time, often spread over days, and therefore costs in the range of \$12 per user.

Acquisition Cost of Passwords

	Passwords			
Product Acquisition	Year 1	Year 2	Year 3	Total
Server Software	0	0	0	0
Maintenance	0	0	0	0
Authenticators	0	0	0	0
Total Acquisition Cost	0	0	0	0

Deployment Costs

	Passwords			
Deployment Expenses	Year 1	Year 2	Year 3	Total
User Initiation	12,000	0	0	12,000
Issuing Tokens	0	0	0	0
Total Deployment Costs	\$12,000			\$12,000

MANAGEMENT COSTS

The final expense, and by far the more considerable, is the ongoing cost to administer and maintain an authentication system. There are two categories of cost incurred when a user encounters an authentication problem. First there is the cost of resources consumed to resolve the problem and then there is the employee productivity that is lost.

Help desk personnel and management time is spent in efforts to resolve common authentication-related problems. These folks also consume telephone resources and use IS facilities to analyze the problem and implement the solution. Meanwhile, the affected user's time is lost and wages and benefits are wasted.

In addition, the productivity of all the people involved is lost during this exercise. To be a good investment to the enterprise, a worker must return value in excess of his/her cost. So when an employee is fully involved in a process to fix an authentication problem, there is the cost of their lost wages, and a lost productivity value of perhaps this much again.

Studies by a variety of consultative and special interest groups have put some values around the costs to fix password-related problems. In one survey, the Help Desk Institute reports that the average, fully burdened help desk cost to respond to one call ranges between twenty and thirty dollars. This includes help desk personnel, telephone charges, management expenses and system costs, but not the expenses of the end user.¹ For our exercise, we will assign an average value of \$25 per call.

It is further estimated that an end-user spends an average of twenty minutes trying to fix a password problem. The first ten minutes are spent trying to solve the problem themselves and the next ten are spent on the phone with the help desk. By assigning a conservative estimate of \$40 per hour to a knowledge-worker's time, the twenty minutes of wasted end user time calculates to approximately \$13 in lost wages and benefits.

Now let's consider the cost of lost productivity. Productivity is defined as the revenue a company would expect to receive from an employee that is above and beyond the cost of their salary and benefits. The end-user lost twenty minutes while the help desk personnel lost another ten. For our example, we will conservatively assume that an employee's productivity value is equal to their fully burdened cost—in this case, \$40 per hour for a total of \$20 for the lost half hour. You can calculate this for your own environment by subtracting the average fully burdened cost per employee from the average revenue per employee.

Management Cost of Passwords²

	Passwords			
Management Cost	Year 1	Year 2	Year 3	Total
Help desk cost	95,000	95,000	95,000	285,000
Wasted end user time	49,400	49,400	49,400	148,200
Lost productivity	76,000	76,000	76,000	228,000
Total management cost	\$220,400	\$220,400	\$220,400	\$661,200

¹ Help Desk Best Practices Survey; 2000

² Password-related help desk costs: 1,000 users X 3.8 calls/yr X \$25 = \$95,000 x 3yrs = \$285,000

Wasted user time: 1,000 users X 3.8 calls/yr X \$13 (20 minutes @ \$40/hr) = \$49,400 x 3yrs = \$148,200

Lost productivity: 1,000 users X 3.8 calls/yr X \$20 (30 mins @ \$40/hr) = \$76,000 x 3yrs = \$228,000

At this point, we can calculate the cost of one help desk call at \$58: \$25 in help desk expenses, \$13 in wasted end user time and \$20 in lost productivity.

One key question remains with respect to this scenario. How often will the typical user forget his/her password and place a call to the help desk?

The typical business year offers numerous opportunities for a user to forget one of his/her passwords. After any extended period of password non-use, such as major holiday periods, vacations and extended trips, a user is likely to forget a password. Certainly, after any password change, no matter how infrequent, many users will forget the new password. If these “opportunities” are compounded by multiple passwords and good password management practices forcing frequent changes, high forgotten password cost is unavoidable. A typical user is likely to average several incidents per year. In a report published by Gartner, the number of password related calls per user per year is estimated at 3.8 using their most conservative scenario.³

The numbers indicate that the average cost per incident of a forgotten password is approximately \$58, assuming the actual experience is limited in the conservative way that we have presented it (e.g., one 20-minute incident). Further, we have learned the average user will call the help desk with a password related issue 3.8 times per year. ($\$58 * 3.8 = \220 per user/per year.)

As we can now clearly see, the real expense of a password management system is hidden in the resources required to keep the system operational.

Total Cost of Ownership Summary

TCO Summary	Passwords			
	Year 1	Year 2	Year 3	Total
Total acquisition cost	0	0	0	0
Total deployment cost	12,000	0	0	12,000
Total management costs	220,400	220,400	220,400	661,200
Total Cost of Ownership	\$232,400	\$220,400	\$220,400	\$673,200

³ *The Cost of a non-automated Help Desk*; Gartner Research; January 14, 2002

Total Cost of Ownership—Summary

When comparing strong authentication technology costs to those of a password system, it is important to look beyond acquisition costs and to consider deployment and management expenses. As shown in this example of a 1,000 user system, it is reasonable to conclude that password management systems can actually be more expensive to own and operate than strong authentication technology systems.

SECURITY EFFECTS THE BOTTOM LINE

When calculating the TCO of a password system, an enterprise must consider security. Weak security can result in immeasurable direct and indirect costs due to exposure of sensitive information and resources to unauthorized users and intruders. Also contributing to the bottom line, strong security may enable business opportunities that result in new or enhanced revenue streams. To this end, we will now explore the impact of *level of security* on TCO.

Relative Security

Determining the level of security needed may seem like a basic step for most corporations, but it is perhaps the one that requires the most attention and consideration. After all, it would be fool-hearty to spend significant funds to protect access to unimportant data or applications, just as it would be unwise to leave critical resources unprotected. It's important to match the solution to the security requirement.

The impact of a security breach can vary widely from company to company as a result of the value of the information that is compromised, the volume of business interrupted, the complexity of the systems and the company's market position.

In Appendix B you will find a list of examples and some questions you can ask to help determine the potential impact of a security breach to your company. Because there are so many variables, it is difficult to put an absolute value on risk. One company may lose very little business, but suffer greatly from employee inactivity. Yet another could experience tremendous losses if their information were to be exposed by a competitor. Carefully considering and answering these questions will help you to determine your risk exposure and help you understand the strength of security that would be most appropriate.

Passwords as a "Security" Mechanism

Passwords are generally considered to be a weak form of user authentication. They can be easily guessed or compromised by someone who is watching or "shoulder surfing" as a user enters their personal information. There are also a number of readily available tools that can be used to crack password files or to sniff data as it is entered through a keyboard and travels across a network. When a password has been stolen or otherwise compromised, the victim usually has no idea their identity has been stolen and the thief is free to act without risk of discovery.

Are these concerns real? The answer is yes!

- It was recently reported by Kevin Poulson of Security Focus that *The New York Times*, a major U.S. news service, had unknowingly exposed sensitive databases to hackers, including a file containing social security numbers and home phone numbers of contributors to their op-ed page.
- In yet another such incident, it was recently reported that computer hackers had cracked into the State of California's personnel database and gained access to financial information for all 265,000 state workers, including Governor Gray Davis.
- And then there is the story of the on-line gambling casino where a hacker gained access to the gaming server, corrupting play so that gamblers could not lose. In just a few short hours gamblers racked up winnings of \$1.9 million dollars.

In 2004, the Computer Security Institute published the results of their annual "CSI/FBI Computer Crime and Security Survey." Based on responses of almost 500 computer security practitioners, the survey is designed to help determine the scope of computer crime in the United States. Once again, it has produced striking evidence indicating that businesses and government agencies are facing high risks and costs associated with network intrusions. Over half of the respondents detected computer security breaches within the last twelve months alone.

As demonstrated by these and many other similar stories, policies that are intended to secure important corporate assets can place these same assets at great risk. And yet, companies continue to incur the costs of forgotten passwords and hope to contain the costs of increasingly likely network intrusions.

Strong Authentication for Enhanced Security

Strong authentication technology can provide a safe and more secure alternative to the use of passwords. The user combines something they know, a PIN, with something they have, a token code from an RSA SecurID token. With this system, it would be impossible for someone to impersonate another unless they had access to both the PIN *and* the authenticator. By combining the use of a patented algorithm, the time of day and a uniquely assigned seed record, an RSA SecurID token automatically generates and displays a pseudo-random token code. When combined with the PIN, the token code becomes the user's pass code allowing access to the protected resource.

PASSWORD CRACKING TECHNIQUES

There are many easy, inexpensive ways to steal user passwords:

Password Cracking Tools. A variety of software tools, such as L0Phtcrack and NT Crack, automate the guessing of passwords through brute force and with extensive dictionaries of frequently used passwords.

Network Monitoring. This technique, also known as "sniffing," allows monitoring (without detection) the contents for any message that streams by and flagging messages based on keywords, such as "login" or "password."

Brute Force Dialing. Programs like ToneLoc automate the process of locating modem telephone lines; then the hacker attempts sign-on with various password alternatives.

Abuse of Administrative Tools. Many tools that have been designed to control and improve networks can be misused for destructive purposes.

Social Engineering. In contrast to the high-tech tools available to uncover passwords, some intruders use non-technical approaches to steal passwords.

THE ROI BENEFITS OF STRONG AUTHENTICATION

There are four significant business benefits that a company may realize by implementing a strong authentication system: increased revenue, lower costs, increased compliance and mitigated risk.

Increased Revenue

The Internet provides wonderful opportunities for companies to do business electronically. By reaching out to new customers, companies are able to grow their businesses faster and more profitably than ever before. But, perhaps the single most inhibiting factor preventing companies from fully utilizing and realizing the potential of this technology is security—more specifically user authentication. In any on-line environment it is critical to establish trust with your customers before conducting business. By first authenticating the user, you can be confident you know the customer is who they say they are and trust that they cannot refute any executed transactions.

We've already discussed the fact that passwords are a weak form of user authentication and that companies should not trust a user's identity based on them. With strong authentication technology, companies can implement e-business applications securely and watch their revenues grow.

Lower Costs

e-Business applications provide the ability for companies to address expensive, labor-intensive internal processes. Order processing, human resource systems, forms processing applications and numerous other personnel intensive business procedures are being automated to introduce efficiencies and reduce costs. As critical components of the business infrastructure, it is important to authenticate users before granting access to these applications. A strong authentication system can provide the user an authentication method that allows companies to implement cost saving business applications confidently and securely.

STRONG AUTHENTICATION

What distinguishes strong authentication from password-based authentication? From a security perspective, the key difference is that a user must provide significantly stronger proof of identity before being granted access to protected resources. Typically, this proof is established by presenting multiple forms of identity or "factors." The more factors a user must present, the more secure an application is considered to be. (Password solutions only require one identifier and are therefore considered the least secure.) Identifiers fall into three broad categories:

- Something only the user knows. This includes passwords and confidential PINs.
- Something only the user has. This is usually a physical device (e.g., a token or smart card) that contains a unique and hard-to-defeat identifier (for example, a one-time authentication code or encrypted digital certificate).
- Something only the user is. This category includes biometric identifiers that are unique to an individual, such as retinal or fingerprint scans.

Historically, two-factor authentication—which is similar to the model established for ATM cards and machines—has been the most common form of strong authentication for users. To prove identity and gain access, an individual must present two factors: a token or smart card and a confidential PIN. As with an ATM card, a criminal must steal the physical device and have access to the user's PIN in order to impersonate that user. This "raises the bar" sufficiently to discourage many identity thieves, who typically will move on, looking for an easier target.

AUTHENTICATION SCORECARD

In planning a strong authentication strategy, an organization can choose from a range of authentication methods and form factors. Different combinations of methods and form factors offer different value propositions in terms of security, portability, scalability, ease of use, reliability and, of course, cost of ownership. For organizations that want to evaluate the merits of different strong authentication methods, RSA Security offers a consistent, structured framework and calculator, the Authentication Scorecard. This vendor-neutral tool, available at www.rsasecurity.com, can help organizations select the most appropriate technologies for their mix of authentication challenges.

Compliance

Concerned with the privacy rights of individuals, government agencies and industry organizations have created legislation and regulations that mandate companies to maintain strict standards to protect personal information. Failure to comply with these laws and regulations can result in significant fines to the offending companies. Further, customers and partners may refuse to conduct business with a company unless it is in compliance with these requirements. By providing strong user authentication before allowing access to critical resources, companies can meet various compliance requirements.

Mitigated Risk

The losses that can be accumulated as a result of a network breach are well publicized. There are daily stories and numerous studies that chronicle the risk facing companies and other organizations. And, as increasingly more valuable data is made available and higher volume transactions are conducted online, the risk continues to grow. Strong authentication can help companies to mitigate their risk by proving the identities of users before granting access to sensitive information and applications.

CONCLUSION

It's obvious that password security isn't really *free*. There are many hidden costs involved—including ongoing management expenses—which are often overlooked when calculating the total cost of ownership (TCO) of such a solution. In addition, one must take into account that weaker levels of security often result in costly breaches, while stronger security enables enhanced revenue opportunities. As a result, there is much to be considered when contemplating the use of password security in lieu of stronger authentication.

This positioning paper and accompanying worksheet will help you understand the actual costs involved in password security. To compare these costs directly with that of a strong authentication implementation, we encourage you to contact RSA Security for comprehensive cost analysis of your unique environment.

ABOUT RSA SECURITY

RSA Security Inc. helps organizations protect private information and manage the identities of people and applications accessing and exchanging that information. RSA Security's portfolio of solutions—including identity & access management, secure mobile & remote access, secure enterprise access and secure transactions—are all designed to provide the most seamless e-security experience in the market. Our strong reputation is built on our history of ingenuity, leadership, proven technologies and our more than 15,000 customers around the globe. Together with more than 1,000 technology and integration partners, RSA Security inspires confidence in everyone to experience the power and promise of the Internet. For more information, please visit www.rsasecurity.com

Appendix A — 3-Year Total Cost of Ownership Worksheet

	Amount	Notes / Hints
Enter the total # users	A	
Enter server software cost	B	Purchase price
Enter annual maintenance	C	One year's cost
Enter cost of tokens, readers, smart cards, etc.	D	Needed to purchase for deployment
Estimate deployment cost per user	E	Consider user request, approval, IT setup, mailing costs, training
Estimate the # of authentication help desk calls per user, per year	F	Gartner reports 3.8 on average
Estimate help desk cost per call	G	Help Desk Institute says \$20 –30 covers help desk personnel & systems
Estimate the average hourly cost per user	H	Include salary, benefits, etc.
Estimate the average end user time lost (minutes per call)	I	20 minutes is common
Estimate average help desk personnel time (minutes per call)	J	10 minutes is conservative
Estimate your company's hourly productivity return per user	K	Expected revenue minus fully burdened employee cost divided by weeks worked and then by hours per week

Calculate acquisition costs	$B + (C*3) + D$
Calculate deployment costs	$A * E$
Calculate management costs, figuring:	
Help desk costs	$A * F * G * 3$
Lost end user time	$A * F * (I/60) * H * 3$
Lost productivity	$A * F * ((I+J)/60) * K * 3$
Three year total cost of ownership	Sum of acquisition, deployment and management costs
Cost per employee per year	3 Year TCO divided by A (# of users) divided by 3 (years)

APPENDIX B — ESTIMATING RISK⁶

Considering the following expenses categories and asking some of these questions can help you establish your company's risk exposure.

Lost business — Companies lose business when systems are unavailable to their customers and sales teams. What would be the cost to your company if you were unable to conduct normal business because your information systems were inaccessible or compromised? Can you estimate how long the systems would be down? How much business does your company normally do in an hour, a day, or a week?

Labor costs — When a system has been attacked, technical resources must be assigned to find and fix the problem. How many people and how long would it take to bring the system back into service? What is the hourly rate of those people? Would there be a need to bring in consultants to help?

Idled users — When a breach occurs, systems are usually shut down and the staff that relies on those systems is rendered non-productive while the IT department tries to contain and repair the damage. How many people would be idled due to unavailable resources? How long would they be idled? What are their hourly rates?

Public relations — It is common that security breaches become public knowledge and companies find it necessary to prepare statements for the press, and answer customer inquiries. Would there be a need to hire a firm to manage the public relations dilemma caused by the breach? If this were to be done by in-house staff, what are the resources your company would expend? What would be the cost in either consulting fees or employee salaries?

Cost of defending the company — Security breaches can result in liability suits due to a failure to protect private information or from the inability to deliver contracted services. Does your company have any contractual obligations that could not be met as a result of compromised systems? Are you subject to any fines due to industry compliance regulations related to information privacy? What would it cost your company to defend itself?

Labor costs of the IT staff and legal representation — To discourage others, many companies choose to prosecute perpetrators of security breaches. Obviously, there are expenses associated with the collection of forensic evidence and the prosecution of an attacker. How long will it take and how much will it cost to find out who invaded your systems? What will it cost your organization to mount a legal case against the offending individual or company?

Customers' loss of trust — Customers rely on your organization's ability to execute business in a reliable manner. Will customers stop conducting business with your company because they don't have faith in its ability to execute transactions or protect private and sensitive data?

Failure to win new accounts — While difficult to measure, damage to a company's reputation can have lasting impact on its ability to attract new customers? Will prospects avoid your company because of negative publicity?

Loss of intellectual property — Critical information in the hands of a competitor can do a tremendous amount of damage. What would be the financial impact if your competitor were to gain access to confidential or proprietary information? Could accounts be stolen? Could new designs be uncovered?

⁶ What Does a Computer Security Breach Really Cost?; Anita D'Amico; SANS Institute; September 7, 2000



RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

RSA, RSA Security, the RSA logo, SecurID and *Confidence Inspired* are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners.
©2004 RSA Security Inc. All rights reserved.

CLHC WP 0804