



What do passwords cost your business?

Investigating the hidden costs in “free” password security

Whitepaper

As companies extend access to their business online, they need enhanced password security, better identity management, and improved remote access control. Unlike traditional password management systems, strong authentication delivers the appropriate safeguards to increase remote access productivity while reducing online risk and the associated operating costs. In this paper, we will explore the total cost of ownership (TCO) associated with the use of password security to allow small and medium sized businesses to make an informed decision about the value of strong authentication systems such as AuthAnvil. We will show that the hidden costs of “free” password security actually outweigh the costs of implementing strong authentication, and offer far less protection.



Copyright © 2012, Scorpion Software Corp.
All Rights Reserved

Table of Contents

| | |
|---|----|
| Introduction | 3 |
| Risks | 3 |
| Reasonable Security | 3 |
| Acceptable Risk..... | 3 |
| Password Security | 4 |
| Are passwords safe? | 4 |
| Is password security really a problem? | 4 |
| The Hidden Costs in Password Security | 5 |
| Acquisition costs | 5 |
| Deployment costs | 6 |
| Management costs | 6 |
| Evaluating the Total Cost of Ownership | 8 |
| Benefits of Strong Authentication | 8 |
| Lower management costs..... | 8 |
| Meet compliance objectives | 9 |
| Reduce risk to acceptable levels | 9 |
| Conclusion | 9 |
| About Scorpion Software | 9 |
| Appendix A – Total Cost of Ownership Worksheet..... | 10 |

Introduction

Much like telephones and fax machines, the Internet is becoming a vital communication medium for small business. As more companies move their businesses and workflow processes to be accessible online, more associated risks become apparent as employees, partners and customers now gain access to critical business resources from anywhere in the world. Compounded with an ever changing threat landscape, some businesses are now evaluating strong authentication to help mitigate these risks to acceptable levels. However, the decision to replace or augment traditional password security systems with stronger authentication can be difficult due to many factors unique to each individual business. One should consider the impact to existing business workflow, and the suitability of the solution within the organization. Evaluating risk against an asset catalogue¹ of critical business resources can help determine if the associated costs in implementing new technical safeguards to reduce risk and protect the business have an effective return on investment (ROI).

Risks

Security is about risk mitigation, and not risk avoidance. It is important that appropriate measures be put in place to reduce risk to acceptable levels for the business. And this is accomplished by applying reasonable security to reduce risk to acceptable tolerance levels.

Reasonable Security

It would be irresponsible to invest significant resources to protect unimportant or irrelevant data and applications, just as it would be unwise to leave critical business resources unprotected. It's important to invest in the right technical safeguards to meet security objectives within the company. What may be reasonable to some businesses may not be reasonable to others.

Much like how reasonable measures of security will differ between businesses, so too will be the impact of a breach in security. It will vary from business to business as a direct result of the value of the information compromised and the volume of business interrupted.

It is difficult to put a dollar value on risk. One business may lose very little in new business from a breach, but could suffer great losses in employee lost productivity. Another may experience tremendous loss if their proprietary information was leaked to competitors or otherwise made available against privacy policies.

Although it may not be easy to place a value on these risks, small businesses can determine their exposure and help understand the strength of security that would be appropriate to offer reasonable levels of security to the business. The goal is to have "enough" security in place to reduce risk to acceptable levels, and give business owners the assurance that they need that their information assets will stay protected.

Acceptable Risk

A company is not in business to be secure; it is in business to be profitable. Derived from its business drivers and impacts, its legal and regulatory compliance responsibilities, and its overall threat profile, each small business has its own level of risk that it is willing to accept.

¹ An *asset catalogue* is an inventory of all information resources and systems that are critical to the business. (ie:Email, CRM, customer databases, documents etc)

The objective is to determine the overall level of risk that the business can tolerate for the given situation. The risk acceptance level is the maximum overall exposure to risk that should be accepted, based on the benefits and costs involved. The traditional security measure for authentication is the password. Is it safe? And if it isn't, is that really a problem? Let's take a look.

Password Security

“Passwords are not only weak, they have a huge problem in that if you get more and more of them, the worse it is.”

- Bill Gates

Are passwords safe?

Passwords are generally considered to be a weak form of user authentication. They can be difficult to manage and hard to remember. Worse yet, because they are so easy to pass around, you don't know if the person actually using the password is who they say they are. Add remote access for these users, and now you have a really BIG problem.

You can think of passwords as a shared secret. And much like any secret, if it gets out, the game is over. Attack vectors ranging from social engineering (“shoulder surfing”) to more complex data sniffing (“key loggers”) make it easy to capture and hold credentials without the user knowing. The victim typically doesn't even know they have been compromised; sophisticated adversaries will utilize their access without you even knowing it.

Is password security really a problem?

You bet! In a recent study² all cases of cybercrime related to network intrusion and data theft prosecuted and publicly disclosed by the *Department of Justice Computer Crime and Intellectual Property Section* that occurred between March 1999 and February 2006. The information collected and analyzed portrays a clearer picture of the attacks and real damages of computer security crimes than has previously been available.

Some of the key findings in this study² showed that:

- Most crimes, eighty-four percent (84%), could have been prevented if the identity of the users connecting were checked in addition to user IDs and passwords
- Losses from stolen IDs and passwords far exceeded damages from worms, viruses, and other attack methods not utilizing logon accounts
- Vast majority of attackers, seventy-eight percent (78%), committed crimes from their home computers; most often using unsanctioned computers with no relationship to the penetrated organization

Based on the responses from over 600 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the “2006 CSI/FBI Computer Crime and Security Survey” (<http://www.gocsi.com>) confirm that the threat from computer crime and other information security breaches continue unabated and that the financial toll is mounting. Patrice Rapalus, former CSI Director explains this best when he says “There is much more illegal and unauthorized activity going

² “Network Attacks: Analysis of Department of Justice Prosecutions 1999 – 2006”

on in cyberspace than corporations admits to their clients, stockholders and business partners or report to law enforcement. Incidents are widespread, costly and commonplace.” This has significant implications for businesses in a whole variety of ways:

- The cost associated with loss of data and information. This includes everything from the cost to recover lost data or information to the more extreme example of having to completely rebuild a data or information set from scratch. This might also include the loss of competitive advantage to others who come to access this lost data.
- The cost associated with lost reputation for breaches of confidentiality. Many, many businesses would suffer huge losses if their customers thought that their confidential data has been accessed – financial institutions and any institution maintaining financial records, and any business that collects credit card numbers are just a few examples.
- The cost associated with a breach of laws, rules or regulations. Many businesses are obliged by law to maintain confidentiality – medical, hospital, legal etc. A breach of their information might also result in legal or regulatory sanctions over and above loss of reputation and customer confidence.

Because of the extremely embarrassing and costly nature of such a breach, these businesses work hard to keep these examples quiet. However, they do happen and happen frequently. Highlights from the “2006 Computer Crime and Security Survey” survey include:

- 52% of respondents detected computer security breaches within the last twelve months.
- 98% of respondents had firewalls installed when they were breached.
- 97% of respondents had anti-virus installed when they were breached.
- 74% of the financial losses were due to viruses, unauthorized access and theft of proprietary information.

Clearly it’s not safe out there. Attackers today are highly sophisticated, well organized and are relentlessly probing weaknesses in network and application security with a specific intent to steal, spy or cause damage. Existing firewall and anti-virus software cannot keep up with the attack of new blended threats taking place in the growing hostile world of the Internet. Insider threats to proprietary information and critical business resources lead to large risks of financial loss, and weak static passwords make it easier for attackers to get in.

The Hidden Costs in Password Security

When considering any security technology to help mitigate risk in a business, look beyond the acquisition costs of the safeguards and consider the on-going expenses associated with the deployment and management of the system. To accurately understand the true cost of ownership of different password systems we will develop a spreadsheet to help calculate the acquisition, deployment and management costs of passwords, considering a three-year period for a business with 25 users.

Acquisition costs

One of the biggest advantages of traditional password systems is that they are typically provided “free of charge” within the operating systems and business applications being used. They generally do not require any extra hardware or software to be used by the end user, and therefore appear to be more cost effective than stronger authentication systems.

Strong authentication solutions such as AuthAnvil on the other hand, require the purchase of hardware authentication tokens and a yearly software subscription for each user.

Remember though that the acquisition cost is only one of three factors that help to determine the real cost of ownership of the solution. The costs to deploy and manage the system must also be considered.

| | Passwords | | | |
|--------------------------------|-----------|----------|----------|----------|
| | Year 1 | Year 2 | Year 3 | Total |
| Software Subscription | 0 | 0 | 0 | 0 |
| Authentication Tokens | 0 | 0 | 0 | 0 |
| Total acquisition costs | 0 | 0 | 0 | 0 |

Table 1 - Acquisition Cost of Passwords

Deployment costs

The cost to deploy different types of authentication systems will vary between solutions. To help estimate these expenses we need to assign a dollar value to the user's time in order to calculate the impact that each solution will have on deployment costs. For the purpose of this paper, we will assume that a typical user's cost (including wages and benefits) to the company will be \$30 per hour, or approximately \$60,000 per year. To meet the unique needs of your own business you can adjust this assumption accordingly in your own calculations in the worksheet in Appendix A.

The first expense that relates to the deployment in passwords is in the creation of user accounts across different systems. Depending on the sensitivity of the information on the system or application being used, this may be as simple as adding a user, or as complex as requiring a full policy management process to be followed. As an example, although it may be quick enough to add a user to an Active Directory system, that same user may also need to be added to the CRM system and have rights assigned to the company intranet. Depending on if the small business handles IT staff in house or through trusted third parties, the typical IT staff cost to the company can be anywhere from \$30 to \$100 an hour. For purposes of this exercise we will assume IT staff cost \$50 an hour to the company. This one-time cost for this user initialization process typically takes a total of 10 to 20 minutes of IT staff time, and therefore will be estimated to cost somewhere around \$12.50 per user.

| | Passwords | | | |
|-------------------------------|--------------|----------|----------|--------------|
| | Year 1 | Year 2 | Year 3 | Total |
| User Initialization | 312 | 0 | 0 | 312 |
| Token Issuance | 0 | 0 | 0 | 0 |
| Total deployment costs | \$312 | 0 | 0 | \$312 |

Table 2 - Deployment Cost of Passwords

Management costs

The last and most considerable expense of password security is the ongoing cost to administer and manage the system. There are two separate categories of expense that need to be considered when managing the system. The first is the lost productivity that occurs when a user is unable to perform their job duties due to an authentication problem. Secondly, we must consider the resources consumed by the company to resolve the problem and implement the solution.

The productivity loss that an employee faces when not able to perform their duties is compounded by the lost productivity that other people involved lose when solving the problem. To be a good investment to the

business, an employee must return value in excess of his or her cost. So when an employee is fully involved in the process to fix a password problem, there is the cost of their lost wages and of lost productivity of perhaps this much again. When IT staff is external to the business, these costs can be even higher when action is needed during no peak times or after hours.

For the purpose of this exercise, we will assume that a single call for support to IT staff (internal or external) will be \$25. This expense covers the personnel and/or consultation charges as well as system charges, but not the expenses of the end user. This corresponds with industry averages, as defined by Help Desk Institute reports³.

We will further approximate that an average end user will spend twenty minutes trying to resolve their password problem. The first ten minutes are spent trying to fix the problem themselves; the next ten minutes are spent working with IT staff to resolve the problem. By using our previous estimate of \$30 an hour for the user's time, the twenty minutes of time consumed costs approximately \$10 in lost wages and benefits.

Now let's consider the cost in lost productivity. In this situation, productivity is defined as the revenue a company will realize from an employee past the expense of their salary and benefits. The user lost twenty minutes while the IT staff lost another ten fixing the problem. If we assign the previous estimate of \$30 an hour as the cost per user, we can expect that a single password issue will cost \$15 in lost productivity for the lost half hour. To calculate this for your own business, simply subtract the average user cost per employee (salary plus benefits) from the average revenue per employee within the company.

From here, we can calculate the cost of a single password incident to be \$50: \$25 for IT expenses, \$10 in consumed user time and \$15 in lost productivity.

While it's nice to know what it might cost to address a single password issue, the real insight comes when we can establish the costs over the year for all employees. To do this we need to know how often a typical user will forget their password and engage IT staff to address the problem.

During the course of a year, a user is exposed to many opportunities to forget their password. After long periods of absence such as holidays and vacations a user may forget their password, or it may timeout and expire. After any sort of password change, there is a good chance some users will forget their passwords. If these opportunities are compounded by strict password policy procedures that force frequent changes, the chance of forgotten passwords will be unavoidable. A typical user will likely cause multiple incidents in any given year. According to some estimates from Gartner research⁴, the number of password related support calls averages 3.8 per user each year, using their most conservative numbers.

From our estimates, we now know the average cost per employee will be somewhere around \$190 per year. ($\$50 \times 3.8 = \190 per user/per year). For our 25 user business example, that's \$4,750 every year!

What can be clearly seen from this analysis is that the real expense of a password management system is in the ongoing maintenance and management of the system. Although it may be free to acquire, considerable expense is spent in order to maintain the system.

³ Help Desk Best Practices Survey - www.thinkhdi.com

⁴ The cost of a non-automated help desk – Gartner Research

| | Passwords | | | |
|------------------------------|----------------|----------------|----------------|-----------------|
| | Year 1 | Year 2 | Year 3 | Total |
| IT Staff cost | 2,375 | 2,375 | 2,375 | 7,125 |
| Consumed end user time | 950 | 950 | 950 | 2,850 |
| Lost productivity | 1,425 | 1,425 | 1,425 | 4,275 |
| Total management cost | \$4,750 | \$4,750 | \$4,750 | \$14,250 |

Table 3 - Management Cost of Passwords

Evaluating the Total Cost of Ownership

When considering the costs of traditional password security it is important to look at the costs beyond the acquisition and consider the deployment and management expenses as well. In many cases, it can be found that in actuality, the price of strong authentication can be more cost effective than that of password security alone.

At the same time, the TCO of strong authentication can show value-added benefits past initial cost savings; enhanced security and threat reduction can also help protect the business from new associated online risk.

| | Passwords | | | |
|--------------------------------|----------------|----------------|----------------|-----------------|
| | Year 1 | Year 2 | Year 3 | Total |
| Total acquisition cost | 0 | 0 | 0 | 0 |
| Total deployment cost | 312 | 0 | 0 | 312 |
| Total management cost | 4,750 | 4,750 | 4,750 | 14,250 |
| Total Cost of Ownership | \$5,062 | \$4,750 | \$4,750 | \$14,562 |

Table 4 - Total Cost of Ownership Summary

Benefits of Strong Authentication

Weak security can result in both direct and indirect costs that may be difficult to measure because of the exposure of sensitive information and access by unauthorized users or intruders. Being able to significantly reduce this threat can be of great value to a small business. Also contributing to the TCO are the new business opportunities that may be available with the deployment of stronger authentication systems that can provide better identity and access control safeguards.

Lower management costs

As we have previously seen, a significant expense of password security is in maintaining and managing user credentials. The use of strong authentication can drastically reduce these expenses by allowing users to never worry about forgetting passwords again. Each time they log onto a system or application that uses strong authentication, they can use their authentication token, in combination with their personal PIN, to generate the passcode⁵ as it's needed.

In areas where passwords cannot be completely replaced with strong authentication passcodes (such as within Active Directory), the management costs can be reduced by allowing the password complexity policies to be relaxed for the traditional password, and augmented with passcodes available in the strong authentication system. This allows small businesses to leverage their existing infrastructure while still adding stronger

⁵ A *passcode* is a combination of a user's PIN and the one-time password generated by an authentication token that can replace passwords in a strong authentication system.

authentication where appropriate... ultimately reducing management costs and increasing the security effectiveness of technical safeguards use.

Meet compliance objectives

To address concerns with an individual's rights to privacy, leading industries and various levels of government have been forced to mandate (through legislation and regulation) strict standards to ensure personal information is protected at all times. Failure to comply with these laws and regulations has the consequence of fines and possible legal action against the offending company. By requiring strong user authentication before allowing access to critical business resources, small businesses can meet the objectives of most compliance regulations and offer assurances that only authorized personnel will gain access to sensitive information.

Reduce risk to acceptable levels

Breaches in security are becoming more common as more companies move many of their business processes online. It is not worms and viruses that are causing the greatest amount of damage, but unauthorized access by untrusted users. By using strong authentication, not only do you reduce the risks of traditional password security, but you *prove* the identity of the user before granting access to critical business resources, and the sensitive information within.

Conclusion

It can be clearly seen that password security isn't really "free". There are many hidden costs overlooked, especially when it comes to the ongoing management expenses that a business must incur to keep the system functioning. At the same time, we need to take into account that weaker security from traditional passwords exposes our businesses to more unnecessary risk. This attracts a greater possibility in security breaches, which can be costly to the company through information loss, productivity loss, or both.

This whitepaper, along with the worksheet provided in Appendix A, will help you to understand the actual costs involved in password security. You can substitute your own numbers to determine if strong authentication costs and benefits outweigh those provided with password security for *your* business. Of course, we encourage you to contact Scorpion Software at any time to get a more comprehensive cost analysis based on your own unique needs.

About Scorpion Software

Scorpion Software Corp provides the premium solution for SMBs to reduce the risks associated with the use of weak static reusable passwords and provide a higher level of confidence that only authorized users can access their company's most important business assets - their proprietary information. Headquartered in British Columbia, Canada, Scorpion Software helps small businesses manage online risk while offering unprecedented password protection. More information about the company is available at www.scorpionsoft.com.

Appendix A – Total Cost of Ownership Worksheet⁶

| | Amount | Notes |
|---|--------|--|
| Enter the total # of users | A | |
| Enter software subscription costs | B | Some vendors may not have a software subscription, but may require you to buy your software separately. |
| Enter authentication token costs | C | Include price of all hardware required (ie: readers, soft tokens etc) |
| Estimate deployment cost per user | D | Consider approval process, IT setup, training etc |
| Estimate the number of calls IT staff may receive in regards to authentication per user, per year | E | 3.8 is the average according to Gartner reports |
| Estimate IT staff cost per call | F | According to HRI, this averages to around \$25 per call |
| Estimate the average hourly cost per user | G | Include salary and benefits |
| Estimate the average end user time lost (minutes per call) | H | 20 minutes is common |
| Estimate average IT staff personnel time (minutes on call) | I | 10 to 15 minutes is conservative |
| Estimate your company's hourly productivity return per employee | J | Expected yearly revenue divided by the number of employees in the company divided by 2000 minus average employee salary and benefits |

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

⁶ Abridged TCO worksheet calculations based on information security risk analysis best practices and formulas provided by RSA Security.