



# **Computer Security For Small Businesses**

**Richard Parrott, MCP  
Microsoft Certified Professional  
COMPTIA A + and Network + Certified Professional**

## **AUTHOR BIO**

Rick Parrott is a Microsoft Certified Professional, and a COMPTIA A+ and Network + Certified Professional with over ten years of Information Technology experience.

Working for several large American insurance corporations and the US Government has given him the opportunity to learn from the best.

Besides working in the Information Technology field, he has taught for vocational schools and the City of San Antonio Adult Literacy program as a network/computer instructor.

Prior to entering the computer field Rick Parrott managed businesses that grossed almost a million dollars a year.

Rick Parrott graduated from Embry-Riddle Aeronautical University in 1994, the same year he left the US Air Force for the civilian sector.

During his Air Force service he worked on C-130 aircraft as a Hydraulic Mechanic and for seven years as an Air Traffic Controller.

Rick Parrott is currently married and lives in San Antonio Texas.

## **LEGAL DISCLAIMER & COPYRIGHT**

© 2006 Rick Parrott. Printed and bound in the United States of America. All rights reserved. No part of this book may be reproduced or transmitted in any form by any means, electronic or mechanical, including photocopying, recording, or by an information storage and retrieval system—except by a reviewer who may quote brief passages in a review to be printed in a magazine, newspaper or on the web—without permission in writing from the publisher. For information please contact Secure Publications, 2459 Cincinnati Ave, San Antonio, Texas 78228.

Although the author and publisher have made every effort to ensure the accuracy and completeness of information contained in this book, we assume no responsibility for errors, inaccuracies, omissions, or any inconsistencies herein. Any slights of people, places or organizations are unintended.

First printing 2006

**ATTENTION CORPORATIONS, UNIVERSITIES, COLLEGES, AND PROFESSIONAL ORGANIZATIONS:** Quantity discounts are available on bulk purchases of this book for educational, gift purposes, or as premiums for increasing magazine subscriptions or renewals. For information please contact Secure Publications, 2459 Cincinnati Ave, San Antonio, Texas 78228. Tel: (210)685-1543

# Computer Security for Small Businesses

Table of Contents

LEGAL DISCLAIMER & COPYRIGHT .....	3
INTRODUCTION .....	7
Chapter One .....	11
Physical Security .....	11
Chapter Two .....	15
PC Security .....	15
STRONG PASSWORDS .....	15
ACCOUNT MANAGEMENT .....	17
BROWSING .....	18
HOT FIXES .....	19
VIRUS PROTECTION .....	19
Chapter Three .....	23
Network Security .....	23
FIREWALLS .....	23
UPDATES .....	24
POLICIES .....	25
BUSINESS CONTINUITY .....	27
CONCLUSION .....	31
Appendix A .....	35
Strong Passwords - Customer Friendly Computer Security	
Appendix B .....	39
Data Backups - One Key to Business Survival	
Appendix C .....	45
Can a Business Continuity Plan Save Your Business?	
Appendix D .....	49
Network Security - Not With a P2P Network!	
Appendix E .....	55
Security, Productivity, and Cost Controls	

# Computer Security for Small Businesses

## INTRODUCTION

Computers have become a necessary part of our personal and professional lives. Everything we do touches a computer in some way.

Overall computers have improved our standard of living. They are however, a double edged sword.

The Internet gives us access to an immense store of information. Need a recipe? What about research for that term paper? Information on

almost any subject can be found on the information super highway.

It can also give us access to an immense store of misinformation. Not all people who put information on the internet are honest. Many have an agenda to further and deliberately twist information to support their objective.

Because of this, more then ever before in history, individuals need to take the responsibility to verify the information they bring into their lives. Explore alternate means of gaining information. Question what you are being told. Then question it again!

Cross reference your information, making sure the information comes from reputable sources.

Another danger we face is loss of privacy. Improperly secured computers can allow others to invade our privacy.

It may not be much of a problem if someone were to access your home computer; but it could be a serious problem if it happened to your business system.

Also, modern technology allows law enforcement and government agencies to scan large amounts of data. They can set the search criteria to alert them when they find what the government is looking for.

The program the National Security Administration (NSA) is using to scan calls from overseas since 9/11 is a prime example. It is designed to alert when it picks up a criteria linked to Al-Qaeda.

In order to secure your data and protect your family you need to close some of the holes into your computer. This ebook gives you the basic information needed to start this process. Using it you should be able to eliminate all but the most difficult problems facing computer users today.

We will cover physical security of your office and computer, then proceed to the security of the PC operating system and finally implement some basic security structures for your network.

These principles apply whether you have a single PC hooked up to the internet via DSL or Cable, or a full fledged office network.

# Computer Security for Small Businesses

## **Chapter One**

### ***Physical Security***

According to industry sources the majority of security breaches are caused by insiders. That makes physically securing your computer systems and network components a high priority task.

When I go into a company and perform a site survey the first thing I look at is the current physical security procedures. How easy is it to get around the current security setup?

Most often there isn't really any security in place. Maybe a receptionist in the lobby, or in rare cases a security guard that walks around the building every couple of hours.

Often getting physical access to the PC is most of the battle when it comes to compromising it. If I can get to your PC with a floppy disk, I can introduce a program that'll help me cause many problems.

I don't even have to log onto the PC. Just rebooting it with an infected disk could do the job!

So what can you do?

1. Start by limiting physical access to your business.
  - a. Your customer's do not need to roam throughout your building.
  - b. Keep them in supervised areas.
2. Institute procedures that require your employees to wear security badges.
3. Define operating policies that prohibit employees from working unsupervised overtime.

## Computer Security for Small Businesses

- a. Don't give employees unsupervised access to your place of business after hours.
  - b. This includes any contractors you may hire.
4. If you can't physically lock up all of your PCs, as in a private office, keep them in a well lit area that is under constant surveillance.
  5. All network hardware should be kept in a secured "access controlled" location.
    - a. In a dedicated server room.
    - b. Or in a specially designed cabinet.
  6. Increase the activity of any security personnel.

Don't forget about your backup tapes! They'll need to be locked up also.

You do perform data backups don't you? See appendix A for a short article on data backups.

Instituting procedures like these will limit the ability of an employee to steal from or sabotage your business. Remember, physical access equals opportunity.

## Computer Security for Small Businesses

## Chapter Two

### *PC Security*

Security at the PC level can be frustrating for you and your systems people. Computer users just want to get their work finished, with as few problems as possible. The challenge is to allow them to do their jobs with as little interference as possible while safeguarding the network.

#### **STRONG PASSWORDS**

Start by enforcing strong password policy. Discourage users from writing down their

passwords and sticking them under their keyboard!

What makes a strong password? Passwords should not be any word found in a dictionary. English or otherwise. They should not be easily guessed. Users should not create passwords that are repetitive. (ie: laser1, laser2, laser3...)

Passwords should be at least eight characters long, non repetitive and include letters, numbers and symbols.

If you are on Windows XP and are using Windows 2000 or Windows 2003 servers use NT File System (NTFS) on all partitions. Older File Allocation Table (FAT) variants did not have the ability to assign file level permissions. What that means is they can only stop access to the whole share, but not to any single file.

It is easier to set NTFS up when you first load the operating system, but it is possible to do later. The command `CONVERT C: /FS:NTFS` will change your FAT21 volume to a NTFS volume. This is a one way only conversion! You can't change it back to FAT32 at a later time.

If you could, you'd lose all of your file level permissions. This would create a gaping hole for a hacker to exploit!

If your network is setup up in a peer-to-peer format then you need to disable file sharing.

In a peer-to-peer network each computer is responsible for its own security. Everyone involved must take security seriously, because there isn't a central point of administrator to ensure everyone complies with security policies.

By disabling simple file sharing you will prevent someone from another workstation from connecting to your PC without authenticating. Computers in a domain format automatically track logons and grant access or deny it based on the access given to the user.

## **ACCOUNT MANAGEMENT**

Account management is a serious issue in either a peer-to-peer or a client-server format. You should


disable the GUEST account and tightly control the ADMINISTRATOR account.

You might even want to rename the administrator account.

Do not create user accounts and give them administrator rights.

Here's one reason why. When you download a virus, that virus will run using the account you are logged onto. If your account has access to everything then the virus has access to everything.

## **BROWSING**

Even though without Microsoft I would not have a job, I feel there are better programs to use when browsing the Internet. My favorite is Mozillia Firefox. And best of all, it's free!  GET FIREFOX

The Mozilla developers take great pride in providing a more secure internet browsing experience than you can get with Microsoft's Internet Explorer.

When I switched from Internet Explorer to Mozilla, I immediately noticed a huge reduction in spyware and adware downloads.

## **HOT FIXES**

Microsoft releases operating system patches called hot fixes whenever necessary. You need to stay on top of these. They are designed to close holes on your system that could let a hacker take control of your computer. You can do this by enabling the Windows Update function from the Control Panel. It's called Automatic Updates. I set mine to automatically download and install the new update immediately.

## **VIRUS PROTECTION**

Next you need to install and update an antivirus program. McAfee and Norton are the big players in the antivirus arena. Make sure you enable the auto update feature! Panda's Security Shield Pro is another excellent "user friendly" security solution for home and office protection.

Malware, another name for virus and Trojan programs, can seriously impact the productivity of your business. It does this in a couple of ways. It can slow your computer system to a crawl or even damage your file system, causing you to lose data!

Related to Virus and Trojans, spyware and adware can infect your system causing slow response times and unstable performance. This type of software is designed to steal or target you for marketing purposes.

You'll need additional software to deal with these intruders. There are several to choose from.

One excellent program is from Lavasoft called Ad-Aware SE. It only runs when you tell it to, instead of running in the background. Programs that run in the background take up system resources that you could be using elsewhere. Ad-Aware SE is free for private use, but not for commercial use. Try Ad-Aware Plus or Ad-Aware Pro.

Privacy Defender is another program that protects your computer from exploitation by adware and

spyware programs. Unlike Ad-Aware, it runs in the background and will detect and clean intrusive programs as they attack your system.

Both programs are effective, however Privacy Defender will protect your computers without your employees needing to remember to run the program.

Now that we have the individual computers taken care of, let's take a look at activities that will help secure your network.

## Computer Security for Small Businesses

## **Chapter Three**

### ***Network Security***

The number one thing you can do to secure your network from external attack is to install a firewall. You need this even if all you have is one PC connected to a modem.

#### **FIREWALLS**

With a hardware firewall, intruders can't even see your network to exploit it. You should still have a software firewall installed to add an extra layer of protection. Companies like Linksys, DLink and

Netgear make firewall routers that you can purchase for around \$50.00.

If you choose to use a software firewall make sure you get one that will allow you to manage data flow. The built in Windows firewall does not allow you to manage flow. Programs like Panda's Security Shield Pro and McAfee allow this control for a very reasonable price.

Most consumer software firewalls use a technique called packet filtering. Data is sent in small pieces called packets. With this technique the each packet is examined and passed or blocked based on the information in the name header. Basically, the firewall asks them who are you and based on the answer approves or disapproves entry.

## **UPDATES**

Like your workstation operating systems your sever operating system needs to be protected and updated. So make sure you update it when necessary and install an antivirus program on it. Be aware though, a standard workstation anti virus program will not work on a server. You have

to buy a program specifically for a server. Norton Corporate Edition is one of these programs. There are others to choose from.

I can't stress how important regularly updating your software is to the security of your network! Just think back on how many times Microsoft's Internet Explorer is in the news for being hacked.

## **POLICIES**

I have waited until now to discuss the two most important activities you can perform to ensure the long term survivability of your network.

First we will discuss security policies. Security policies are nothing more than rules. These rules tell us actions are allowed or disallowed on our network or computer.

When you tell your son that he can't surf porn sites you are setting an acceptable use policy. Likewise, when you tell your employees they can't surf porn sites, you are setting an acceptable use policy. In both cases the policies are designed to offer protection from harmful activities.

American courts are fast catching up with the internet age. They are increasingly holding companies accountable for the actions of their employees on the internet. How can you protect yourself?

A good place to start is with; you guessed it, security policies. Start with an Acceptable Use Policy. This will establish the basic guidelines that your employees will use to perform their duties on your computers. It will also give you a little protection if your employees are doing anything illegal. Maybe even enough to save your business if you are sued.

Additional security policies can further define the limits of behavior on your network. Remember, the goal here is to decrease the risk to your business.

To ensure that your security policies are adequate to protect your business you should engage the services of a competent IT security professional.

## **BUSINESS CONTINUITY**

Business Resumption Planning (See appendix) should be an important part of your overall business planning. This planning shouldn't just be limited to things caused by nature, such as floods and earthquakes. It should encompass every facet of your business.

The cornerstone of your business resumption plan is establishing a credible data backup policy, and executing it. After all, what good is it to save your business only to lose it later because you had lost your customer data?

Ask yourself this question. How long could my business survive if all of my customer data were lost? Consider everything from marketing to maintenance files to warranty information.

Yes, a full blown disaster recovery plan can be an expensive undertaking. If you can't afford it, there is a way to spread the costs out over time.

A Critical Resource Recovery Plan targets individual parts of your business and develops a recovery procedure for each section. Each part is

assigned a priority and then developed. After all the parts have been developed, they are then tied together into a comprehensive plan.

This method will result in a higher total cost, but may well be more affordable. Sort of like an installment plan.

As a minimum you should at least perform daily backups. There are many software programs that will allow you to safeguard your customer data.

Starting with the free backup utility built into the Windows Operating System. Unfortunately, the Windows Backup Utility is a bare bones utility and has to be setup on each computer you want to backup. Also, it is not included on Windows XP Home Version.

For a network solution try one of these software programs:

[Vision Backup 10 – Enterprise](#)

[WinBackup 2.0 Standard](#)

## Computer Security for Small Businesses

Remember, the most important thing is to back up your data! Do it! Do it everyday!

## Computer Security for Small Businesses

## **CONCLUSION**

We have briefly touched on actions you can take to increase the security of your computer network.

While many of the suggestions contained within this document may seem simplistic, they are effective. Advice such as locking the door to your server room could seem insulting, but many times I've encountered just this problem when performing a site survey at a client's office.

Computer and network security isn't rocket science; instead it is the application of the same

common sense you bring to other areas of your life. Sure you may need to know how to implement the more complicated configurations, but that's what you pay consultants for.

Sit down, right now! Pull out a piece of paper and a pen. Walk around your office and note the security problems you find. Then walk around the office again and see what can be changed to increase the security of the area.

It may mean moving desks, cabinets and computers to ensure that you can see everything that goes on in the office. At home it might mean moving the computer from the bedroom to the family room.

Whatever you find it will assist you with you site survey. Then move on to you computers. This will take some time to do properly; many consultants will do a preliminary consultation for free.

Systematically work your way through your business: when you are finished you will have greatly increased your businesses ability to prosper.

## Computer Security for Small Businesses

If you feel you need professional assistance, any competent network consultant can perform a site survey for you.

Look at it as an investment, not as a cost.

## Computer Security for Small Businesses

## **Appendix A**

***Strong Passwords - Customer Friendly  
Computer Security***  
**Article Reprint by Rick Parrott**

## Computer Security for Small Businesses

### Strong Passwords - Customer Friendly Computer Security By Rick Parrott

Go into to any office and look under the computer keyboards and you'll eventually find a little piece of paper with that users logon ID and passwords. Probably every password that person has.

This illustrates a serious problem with the use of networked computers in business. User apathy and IT security arrogance often combine to defeat the purpose of established security policies.

What happens is that IT security policies clash with usability. Most customers will not follow policies they see as too difficult. One place IT policies and user compliance clash is at the point of entry for any secure computer system. The logon screen.

First, let's agree on a definition for a strong password.

From Webopedia, A password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized. A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, \$, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or parts of the user's own name.

Customers will not use difficult passwords. Sorry, they just won't! For instance, you have two passwords: 1Xc%&27m3 and parrott5. Which is the strongest? Which do you think your customers will use?

## Computer Security for Small Businesses

The key here is education. End-users must be educated on the seriousness of computer security and IT security professionals need to be aware of the needs of their user base.

You should avoid sequential passwords: parrott1, parrott2, parrott3... You should use a password that is easy to remember, but not in any dictionary. Maybe combine parts of two words, adding capital letters and numbers.

IT security professionals may not like this compromise, but it is better than passwords that are easily broken.

Strong passwords are critical to the security of any computer security, but are they the best way to control access? In part two, we'll look at alternatives to passwords.

## Computer Security for Small Businesses

## **Appendix B**

### ***Data Backups - One Key to Business Survival*** **Article Reprint by Rick Parrott**

## Computer Security for Small Businesses

### Data Backups - One Key to Business Survival

By Rick Parrott

Your customer data is a precious resource that can literally be worth its weight in gold! If used properly, it can be mined over and over for additional sales and referrals. Do you use this gold mine to increase the profitability of your business?

You should! It can mean the difference between business survival and failure.

Why then do so few business owners take the time to ensure that it is adequately protected? Are we too busy? Perhaps you just didn't know how to protect it, or couldn't afford the software and hardware required to back up your data correctly.

Ask yourself these questions:

Is there anything more important to my business than my customer data? What would happen to my business if I were to lose all of my data?

Consider this common scenario. A client calls frantic that she'd lose her business if she couldn't recover her customer data. She had over five years of information on her computer when the hard drive decided to make her life interesting.

So what are her choices? Renter the data manually, if she has any hard copies available. Call everyone and ask for their contact information again, won't that make them feel secure about her company. Or call a data recovery technician. Their services can start at a thousand dollars and go up rapidly from there!

## Computer Security for Small Businesses

Windows XP provides a fully functional backup utility, for free! In fact, many of the commercial backup products use this backup to save the data. All you are paying for is the user interface, the window you enter information into.

Before you run the setup wizard, you need to answer a few questions.

What data do I need to backup?

Only backup data that is necessary. Use the KISS (Keep It Simple Silly) method. Your customer database and correspondence should be backed up as a minimum.

How often do I want to back up my data?

How often does your customer data change? Does a significant amount of data change on a daily basis? Weekly?

Where do I want to store my data backup?

Most data backups still use a tape drive to store the data. The problem is that they cost a fortune! The tapes alone are expensive. Alternatives are to store your data backup on another computer on your network or copy it to a CD or DVD writable disk.

Ok, so you want to backup your data. What now? Before we do that review the table below:

### **Full Backup**

- \* Copies and stores a complete duplicate of your data every time it runs.
- \* Takes the most time to run and the most storage space.
- \* Quickest data recovery feature.
- \* Easiest!

### **Incremental Backup**

- \* Copies and stores only data changed since the last backup.
- \* Must be combined with a full backup, and any other incremental backups.
- \* Most complicated.

### **Deferential Backup**

- \* Copies and stores data changed since the last full backup.
- \* Must be combined with a full backup and the last deferential backup.
- \* Middle of the road.

If you have a relatively small amount of data, I would suggest a daily full backup. If you have a larger amount of data you might combine the full backup with a deferential backup. Simple huh?

The next question is how to store the data backup. Even though it takes a little extra work, I have my clients back their data up to a DVD writable disk. First, set the wizard to back the data up to a folder. Usually this folder is on another computer. Then burn this data to a DVD burner and place the disk it in a secure location for retrieval as necessary.

If you don't feel comfortable setting this up yourself, any competent PC technician can do it for you.

Whether you do the setup yourself or have it setup by a professional technician you are taking the first step in ensuring the long term survival of your business. Please take the time to do this.

Ultimately your customers don't care how or why you lost their information, they just care that you did. I'll leave you with this statistic:

## Computer Security for Small Businesses

Estimates suggest that 80% of small businesses that suffer a serious computer failure cease trading within two years. Will yours be one of them?

## Computer Security for Small Businesses

## **Appendix C**

### ***Can a Business Continuity Plan Save Your Business?***

**Article Reprint by Rick Parrott**

## Can A Business Continuity Plan Save Your Business?

By Rick Parrott

Think about it!

When you start a business you create a business plan. When you want to bring a product to market, you create a marketing plan.

Doesn't it make sense to create a Business Continuity Plan to save your business? Of course it does!

Not every business disruption is caused by a major disaster. In fact, most are caused by everyday problems.

The night maintenance crew accidentally unplugged the server. An employee attempted to access a database that was being upgraded and corrupted the information it contained. Or the transformer down the street blew up during a sudden thunder storm.

In each case, your company could have been negatively impacted!

A solid business resumption plan would have predefined your responses to any of these situations. In fact, it would have helped you avoid the first two and greatly reduced the impact of the last.

Consider these statistics:

- 52% of American companies have had operations seriously interrupted because of computer hardware problems...
- 43% American companies have had operations negatively impacted because of problems with their software...

## Computer Security for Small Businesses

- 34% have had business operations seriously interrupted because of human error...
- 75% of companies impacted by a serious catastrophic event fail within two to five years...

Yes, a good business resumption plan is a time consuming project. Yes, you do not have enough time for the projects you already have. Much less the time to take on something new!

Ask yourself these simple questions.

1. What would happen to my business if all of my customer data were destroyed?
2. What would happen to my business if my building was flooded or destroyed?

If the answers to questions like these have only negative outcomes, then you need the services of a professional Business Continuity Planner.

Call one now!

## Computer Security for Small Businesses

## Appendix D

***Network Security - Not With a P2P Network!***  
**Article Reprint by Rick Parrott**

## Computer Security for Small Businesses

### Network Security - Not With a P2P Network!

By Rick Parrott

Most small business networks grow and evolve as the business grows. In one way, this is good. It shows the business is growing, becoming stronger. Unfortunately, from a network perspective, it can be a disaster in the making.

Most small business networks are setup in a peer-to-peer (P2P) format. In contrast, large corporate networks are setup in a domain format. What does this mean to you?

First, let us define the two network formats. In a P2P format every PC is responsible for its own security access. Basically, each PC is equal to every other PC in the network. These networks generally consist of less than ten computers and require a large amount of administrative overhead to function securely.

In this format the attitudes of the user population is of prime importance. If they have a high level of security conscience then your network will be more secure, if they don't your network will be wide open to insider exploitation.

You can see the problem. Ten computers and ten administrators equal little accountability.

In a domain system there is a single point of administration, your network administrator. He is responsible for maintaining the network.

A network setup in this format consists of at least one server, a domain controller, to administrator the rest of the network. This domain controller manages user and computer access, freeing the

## Computer Security for Small Businesses

network administrator from the necessity of touching every PC in the network.

When a user logs onto her PC in a P2P network she only authenticates on it, in a domain system it is a little more complicated.

In a domain system she logs onto her computer, her login ID is first checked with the domain controller. If it is found she is granted access to the network resources assigned to her. Then she is allowed to log on to her desktop. If her ID isn't found then she only has access to her local PC.

Now that you know a little about the two network structures you can see the advantages of the domain design.

As stated earlier this format requires planning to achieve. You must sit down and outline what you want your network to accomplish.

Consider what access your users really need to do their jobs. In the computer security world this is called granting the least amount of access required to do the job. Do your sales reps really need access to your financial files? What about external vendors?

All of this needs to be thought out and addressed.

Here's an example of how I setup a small sales organization. This business consisted of about eight employees and the two owners. With the assistance of the owners we defined three user groups.

The owners group was granted full and complete access, while each of the other groups received lesser and different accesses. The admin group received access to the financial and administrative functions, and the sales groups receive access to the sales and

## Computer Security for Small Businesses

customer management data. Specifically, they were excluded from the financial and administrative and the owner's functions.

Additionally, we setup auditing of both successful and unsuccessful attempts to view certain types of data. We did this to add a layer of accountability to the network. This increases the security of their customer's data because we can now tell who and when the data was accessed.

Network security personnel know that most network security breaches occur from the inside! In my experience most small businesses use the P2P format because it is the easiest to implement and because they don't know the security compromises they are working under.

This can be a ticking time bomb for your business. Eventually, you will experience a security lapse that could land you in court.

For instance, you have an employee leave your business. This employee downloaded all of your customer data before he left. Next, he sells this data to someone who uses it to steal the identity of several of your customers. Eventually, this theft is discovered and traced back to your employee.

Your former customers in fully justifiable outrage take you to court charging you with negligence. Specifically, they hold you responsible for failing to safeguard their personal information.

Your case will be much stronger if you can show you have positive control of your network. You can point out your security procedures. Employee logon auditing, security updates, acceptable use agreements, etc. In short you can show that you have taken the steps that a reasonable person would take to secure your network and customer data.

## Computer Security for Small Businesses

Hopefully, your lawyer can then place the blame directly where it belongs. On the employee who stole the information in the first place. Ask you attorney about this! Don't just take my work for it, I'm not a lawyer.

Remember, network security is a result of through planning, not hap hazard improvisation. Give your network the same attention you give to the rest of your business.

If you do not have the skills or the time to be your own network administrator, you can contract with someone to handle this for you on a part-time basis. Just make sure they are reputable, you are putting your business in their hands.

## Computer Security for Small Businesses

## **Appendix E**

### ***Security, Productivity, and Cost Controls*** **Article Reprint by Rick Parrott**

## Computer Security for Small Businesses

### Security, Productivity, and Cost Controls

By Rick Parrott

Go ahead; mention computer security to the average small business owner. See how fast his hand covers his wallet. This is because most people see security as an expense. The average small business owner immediately thinks about the costs to implement something, not necessarily how it will help his business.

Of course, this reaction varies on the number of security incidents the small business owner has experienced. It is amazingly easy to convince a client to install a backup system after he has lost his entire customer database.

So what do we do? Nothing in the business world exists in a vacuum. Especially security, we need to look at security as an enhancement to the business. Not just as an expense.

Security can be a somewhat vague concept. So let us break it down into segments and define what it really means.

Physical security is the actual measures you take to protect your premises and equipment. It could be putting locks on your doors or hiring a security guard to control access to your building.

Information security means taking actions to safeguard your data, both electronic and printed. This consists of adopting security policies and imposing an electronic authentication and control system on yourself and your employees.

All of this enhances productivity by creating an environment that functions smoothly.

## Computer Security for Small Businesses

Clearly defined security practices are necessary to avoid over control. These practices can greatly enhance the productivity of your employees by reducing down time.

Security professionals need to balance the need for securing the network against the possibility of hindering productivity. In the real world, security can be too tight.

All it takes is one virus to demonstrate how security vulnerabilities can destroy productivity.

Another of the benefits to implementing a quality security program is the increased ability to control costs.

In the planning stages, you need to gather information on all of your vulnerabilities and assets. A good inventory plan will be necessary to complete this stage. Once finished, it will assist you with managing your resources.

A through business survey will identify areas of your business that need improvement and areas that perform especially well. Knowing these strengths and weaknesses will allow you to allocate funds with more certainty.

Growing a business is not just about getting new customers or keeping the ones you have. It is also about managing your resources and controlling costs. Asset management is a big part of this.

How much control do you have over your business? Are you spending money in places you shouldn't? How do you know?

Look at security and inventory control as a means of enhancing or managing your cash flow. Almost 40% of small businesses fail every year because of cash flow! Will one of them be yours?

## Computer Security for Small Businesses

As a small business owner you must, yes must, accept that computer security is necessary in this day and age. Failure to implement a strong security program leaves your business open to exploitation and compromise.

Right now, go online or to the yellow pages and find an IT consultant to assist you with securing your business. Do it now!