



Securing Data in a Small to Medium Size Business

A Practical Guide to Business Data Security

Securing the Small to Medium Business







About the Author

Joseph A. O'Donnell, President and Founder

Mr. O'Donnell is a hands-on Owner. He is familiar with the technologies, the costs and the people in the data security business, who brings 15 years experience working with senior level executives and Fortune 500 companies, as well as with small and mid-sized businesses.

Before founding Data Security Solutions, Joe founded several successful telecom and IT companies and currently also owns and operates PC SWAT. He was the principal author of United Technologies and Otis Elevator Company's Conferencing Portal. Joe delivers expertise in software architecture, and he has created multiple databases for Fortune 100 Companies to manage their telecommunications departments.

As a nationally known technology expert, he has been quoted in the following:

-  *Wainhouse Research Bulletin*
-  *Teleconferencing Business*
-  *Telecom Newsletter*
-  Polycom Corp's Web Site
-  *The Boston Herald*
-  *The Boston Globe*

He is a frequent guest speaker and panelist and is the author of "The Anatomy of Web Conferencing Choices and Migrations," published in the *Web Seminarian*, and the co-author of "Riding the Web Conferencing Tsunami", an extensive industry report on web conferencing and related markets with Wainhouse Research.



Securing the Small to Medium Business

Introduction	4
The Data Security Problem	5
Local Backup Solutions	6
Off-Site Backup Strategies.....	7
Network Security Implementation.....	8
Software Encryption	9
Power Source Protection	10
Conclusion.....	11

Securing the Small to Medium Business

Introduction

Internet and email technologies have become critical tools in the small to and medium-sized business world, presenting opportunities for increased efficiency, flexibility, and communications. However, the same open architecture that allows for those gains also presents risks.

This blessing and curse quandary places stresses on the business community. New threats from a variety of sources arrive daily, and it seems impossible to account for and defend against all of them. Of course, there are reasonable measures that can be taken to insure the safety of your business data.

This white paper will discuss the main source of threats and practical ways to avoid a business disaster.

Securing the Small to Medium Business

The Data Security Problem

The 2004 *Computer Crime and Security Survey* published by the FBI and Computer Security Institute shows just how pervasive security threats are for organizations:

- 88% of respondents detected computer security breaches within the last 12 months
- 74% acknowledged financial losses due to computer breaches
- 72% of respondents cited their Internet connection as a frequent point of attack, up from 59% in 2000
- 38% of respondents cited their internal systems as a frequent point of attack

According to a recent study by PriceWaterhouseCoopers, the worldwide loss of revenue due to security breaches totaled \$1.4 trillion.

Another PriceWaterhouseCoopers study shows that 70% of small businesses that have a major data loss will be out of business within the year. Each year 25% of all PCs will have a data loss. Ninety-six percent (96%) are never backed up.

Add to this the fact that smaller firms, those with 5-200 employees, typically do not have dedicated staff to keep up with the changes in security threats. The typical business has a relationship with an “IT guy” that is usually termed a “break-fix” guy. For example, “my email is not working,” “my computer won’t start,” etc. They are rarely consultants that evaluate your business from a data security perspective nor are they likely to be schooled in that specialty. This leaves the small to medium-size business in a vulnerable position from the myriad threats that can stop business all together. Data Security Solutions has identified 5 major points of data vulnerability.



Securing the Small to Medium Business

Local Backup Solutions

Small to medium-size businesses are typically more narrowly focused, with smaller budgets and no in-house expertise in the area of data security. This leads to security vulnerabilities. One major source of vulnerability is local backup.

All too often businesses are using tape backup. Tape is unreliable. Industry data shows that 50% of the tape backups are not useable. Floppies and Zip drives can be worse. All are subject to data loss and human error. And, if yours are like most organizations, you never test to see if the data are valid. In addition, tape backup restoration procedures can be up to 400 times slower than recovering data from a disk. Most taxing is the cost and effort it takes to administer tape backup systems, rotating tapes, checking them and transporting them offsite.

Businesses not using tape, CD, or Zip drives are likely relying on cheap sub \$200 hard drives that have no internal cooling mechanism, making the average life span far shorter than high quality hard drives, which can last for 10-20 years.

Data Security Solutions recommends at a minimum:

- Hard drives with a metal casing assembly (not plastic)
- Hard drives with an internal cooling mechanism to provide optimum operating temperature for long life such as our GT 050Q 7,200 RPM Hard Drive.



Securing the Small to Medium Business

Off-Site Backup Strategies

If a large number of small to medium-size businesses have inadequate local backup, a far greater number do not have a reliable off-site backup system. Most have no system in place and are at severe risk to natural disasters (fire, flood, etc.) and malicious viral infections that can destroy critical business data. For example, with no reliable off-site backup system in place, a fire could destroy a business. The cost to that business is incalculable, yet many take the risk.

An off-site backup strategy involves two primary components:

1. A reliable software system that backs up all of your data to a data warehouse on a schedule
2. A reliable and secure data warehouse with 99.999 uptime where the data is stored.

Unfortunately, some off-site backup providers claim to have the safeguards in place that can guarantee companies recovery of their business data, but do not in fact take the measures necessary to ensure that your data will be available in case of disaster.

Some of the measures that should be in place for any off-site backup facility are:

- Secure bank-level encryption employed when transferring data
- Multi-diesel generator power backups for the data warehouse
- Biometric (hand print, voice print) physical security allowing only authorized employees within the data warehouse
- A software tool to restore your data in an easy automated fashion, should disaster occur
- Triple level authentication for access to your data in the warehouse (username, password, and one more authentication procedure).

Data Security Solutions offers off-site backup that meets these stringent requirements. Our “set it and forget it” approach allows companies to focus on the important things, such as sales and service.



Securing the Small to Medium Business

Network Security Implementation

Some businesses rely on inexpensive and poorly made router hardware that lacks the necessary tools to protect their network and their data. In fact, the majority of small to medium-size businesses are setup only to wait for network attacks, then hope their anti-virus software is working, is up to date and able to extinguish the threat.

Unfortunately, this approach leaves businesses with a critical vulnerability. For example, there are viruses that pass through an inexpensive router undetected using a common Internet access point, then take secure control of a PC or server and cannot be extinguished by anti-virus software. Once a virus is able to run in memory and gain certain access rights, anti-virus software on that PC or server is rendered useless.

Data Security Solutions recommends the purchase of routers that have built-in anti-virus, anti-spyware, and network intrusion detection. This approach means there is now a guard at the door of the business instead of waiting until the breach has occurred. Anti-virus and anti-spyware “at the door” destroys threats long before they touch a single PC or server in your business. Network intrusion detection examines in high detail every data packet going in and out of your business. Any data packet flagged as malicious or suspicious is stopped “at the door.” All Data Security Solutions routers have up to date anti-virus, anti-spyware, and network intrusion detection protecting your business in real-time before it is too late.



Securing the Small to Medium Business

Software Encryption

If the number of small to medium-size businesses implementing off-site backup is small, then the number employing encryption technology is even smaller. Nearly every week, the news reports another laptop stolen that had credit card numbers, or a computer was stolen with Social Security numbers, etc. If those computers had employed data encryption solutions, then the data on those computers would be useless to those who stole them. Yet, too many businesses store sensitive data on computers that can be easily compromised by employees, hackers or thieves.

There are two primary forms of data encryption: hard disk sector level and file or folder level encryption. Hard disk sector-based encryption encrypts the entire hard drive, rendering data completely undecipherable to unauthorized users. File or folder based encryption allows a business to specify which files or folders should be encrypted. For example, a simple form letter to a customer would not be encrypted but the company customer database would.

Data Security Solutions offers both hard disk sector-based and file or folder encryption solutions. In addition, our encryption solutions offer pre-boot authorization protection. This process creates a separate part of the computer where users log in that is unreachable by any hacker. This ensures that disk data remains encrypted and hack-proof.



Securing the Small to Medium Business

Power Source Protection

One area of data security not often thought of is power protection. The majority of small to medium-size businesses use simple surge protectors to defend their businesses from power fluctuations, power loss, or damaging power spikes that can destroy a computer and all the data in it. Contrary to common belief, surge protectors are completely inadequate for protecting electronic equipment. They cannot regulate power fluctuations, do not provide for battery backup in case of power loss, and cannot stop serious power spikes that will damage electronic equipment and mission critical data.

Data Security Solutions recommends that businesses employ only uninterrupted power supplies to protect their businesses from power problems. Uninterrupted power supplies protect electronic equipment from any power fluctuation, warranty their protection, assign battery backup when power is lost, and offer powerful management software to monitor power conditions and gracefully shut down applications and computers in the event of power failure.

Data Security Solutions deploys top of the line APC (American Power Conversion) power protection solutions, including customized software management setup tailored to your business.



Securing the Small to Medium Business

Conclusion

Lack of education is the primary reason for the woeful state of data security in the small to medium-size business community. Most businesses are understandably concentrating on day-to-day issues and are not focused on long-term strategies to maintain business continuity. Data Security Solutions is committed to bringing the best, most affordable technologies and expertise to secure data for the small to medium-size business community. Deploying strategies like those discussed in this paper will ensure that business data is secure and the business will not suffer a deadly blow that can bring a powerful end to profitability and have a disastrous impact on customers.

To find out more on how Data Security Solutions can help your business, contact us toll free at 877-651-7032, email us at info@datasecuritysolutions.net, or visit our web site at www.datasecuritysolutions.net.

