5 DEADLY MISTAKES THAT BUSINESS OWNERS MAKE WITH THEIR COMPUTER NETWORKS AND HOW TO PROTECT YOUR BUSINESS

Agility Networks, LLC

Introduction

As small and mid-sized companies rely more heavily on their computer networks to conduct nearly every aspect of their business, it's more important than ever for those computer networks to be extremely well managed, updated and secure from external threats. Some companies are entirely dependent on their networks to deliver their products and services. For those companies, if their networks go down, they are effectively out of business until the network can be restored.

Yet many small companies are taking risks with their networks and by extension, their entire business, and they often aren't even aware of it. Agility Networks has been providing computer network support services to Chicago area businesses for over 11 years. Based on hundreds of interviews and network surveys, this special report documents the five most common and most dangerous risks that business owners take with their networks and provides practical advice on how to avoid those risks.

1. YOU HAVE A FIREWALL, SO YOUR NETWORK IS PROTECTED, RIGHT?

Probably not. The router that came with your high speed internet connection or that you purchased from a computer store probably has a rudimentary firewall built into it. The problem is that the firewall is usually not sufficiently configured, managed, monitored and maintained. The reason it's a problem, is that the people who are attacking your network 24 hours a day, 7 days a week have access to very sophisticated "hacking" tools. Both the sheer number and the power of these tools have increased dramatically just in the last six months. Hackers now have available to them tools that are hundreds of times more powerful and more sophisticated than ever before. This phenomenon has many network security professionals alarmed. If you doubt this for one moment, type the words "hacking tools" into Google and look at the list of thousands of freely available tools.

Firewall protection is one of the most important pieces to the network vulnerability puzzle. Although your server may not be a target by any one person or entity from a hacking standpoint, it is the non-targeted; brute-force broadcasts that hackers unleash that can cause the most common and serious problems.

A sophisticated hacker is an expert at discovering ways to penetrate network devices that are not correctly updated, managed or improperly configured.

- **A hacker isn't necessarily after your data; typically a hacker will use your hacked server as a launch pad to attack another server or as a spam relay. In either case you won't know about it until it is much too late and the business risk is staggering.**

Here are just a few of the consequences of what can happen if you are the victim of a hacker's broadcast attacks. These don't even take into account what can happen if you are the victim of a targeted attack.

- **A hacker makes your server a spam relay.**

ISP's now have a strict policy of not accepting any email from a server that is a known spam relay. All of your outbound email simply stops getting delivered. In the best case, you will be notified that your company is now a known spam relay and no company will accept email from you. In the worst case, you won't.

- **A hacker makes your server a launch pad for attacks against other servers.**

Depending on who your hacker decides to attack, the consequences can range from bad to catastrophic. If your hacker decides to attack a major American pharmaceutical corporation, you will in all likelihood receive a visit from local law enforcement personnel. However, if your hacker decides to attack a government or military agency, you will likely be visited by the federal authorities. They will shut down your server, and probably your business, while their forensic IT experts determine your level of involvement. Not surprisingly, they will be incredibly slow, thorough and careful in their investigation as they tend to take these matters quite seriously.

- **A hacker turns your server into a public FTP site.**

Your server suddenly becomes home to any number of viruses, spyware or other types of malicious software. From there it just gets worse. A public FTP site can also be a home for truly illegal activities for which you may have legal if not criminal responsibility.

Is it worth it to have a professionally configured, managed, monitored and updated firewall?

---

2. HOW CLOSE IS YOUR BUSINESS TO DISASTER? A SIMPLE TEST TO FIND OUT

All small to mid-sized firms know they have to back up their data and most do. However, few have ever tried to restore their data to see if their back up strategy is really working until disaster strikes, and by then it's too late.

Many companies can't run their businesses without their computers any more than they can run their business without phones or electricity.

- **Yet here are the alarming facts. Nine out of ten small to mid-sized businesses never test their backups.**

Eight out of ten small businesses don't even have a documented backup procedure that protects their business.

The simple fact is that most small to mid-sized companies are exposing themselves to business risks that they would deem unacceptable, if they were aware of it. Fortunately, creating an effective backup procedure is an easily accomplished task for a technical professional.

Even companies who have made the effort to develop a well thought out back up plan and execute that plan consistently often make the crucial mistake of not testing their backups

To use a real world example of how important it is to test backups, we'll use the case of a real Agility Network's customer. At the first meeting, Agility Network's consultants asked the new client about their backup procedure. The client described a well thought out backup procedure that they had developed and faithfully carried out.

However, during a routine review of the company's back up logs, it became obvious that the backup software they were using had malfunctioned – it appeared to be making a backup, but it wasn't. Since the company had never checked their backup logs and they never tested their backups, this company had failed to backup 6 months of data.

If their server drive had failed, this architectural firm would have lost 6 months of nearly completed client work and 6 months of billing and accounting records. Without this critical data, the company probably would have been on the brink of bankruptcy.

- **How to develop an effective backup plan.**

Agility Networks recommends that an effective backup plan be completely documented, with written descriptions for daily, weekly and monthly backup procedures as well as frequent testing procedures.

An effective backup plan saves data apart from a production server so that files can be restored quickly and easily. If tapes are used, they should be moved off-site, so that data can be restored in the event of fire, flood, theft or other catastrophe. Tapes should be rotated and replaced frequently. Tape drives should be cleaned at least once a month. Full backups of all system data and incremental backups need to be scheduled appropriately.

Incremental backups, which backup only the data that has changed since the last backup, should be done more frequently. Incremental backups decrease the business risk of data loss because it shortens the time between the last backup and the failure. However, every business needs a strategy that balances the frequency of full system backups and incremental backups.

Backup procedures should be automated to decrease business risk that can result from human error. Agility Networks recommends having a network backup automation solution. It should be a professional-grade software product that is easily managed and provides detailed records and information about every backup.

- **It's not a technology question, it's a business question.**

How long can your computer system be down before it begins to have serious financial consequences for your company?

- **How long can your systems be down before it has some impact on your customers?**

- **The instant your network failure inconveniences your customers is when your risk of losing valuable customers skyrockets.**

They may stay with you for a while, but they may also start actively looking for a new vendor or supplier of the products or services you provide. In today's business environment, customers have little or no tolerance for mistakes. One simple mistake can give your customers a reason to look elsewhere to obtain the goods and services you provide.

The answers to these questions vary depending on the type of business you own. Some information-intensive financial services firms cannot afford to be down for even a few minutes. Other companies that are more human labor intensive can afford to be down for a day or two before it impacts their customers.

- **Minimizing Business Risk**

After the safety net of a stable, tested and documented backup solution is in place, it's important to take appropriate steps to reduce the likelihood of critical equipment from failing in the first place. One simple step to reduce the likelihood of needing to restore from a backup is to utilize an inexpensive and highly effective technology called RAID, which stands for Redundant Arrays of Inexpensive (or Independent) Drives.

A RAID solution means having multiple disk drives mounted in the server and controlled by a combination of hardware and software. With a RAID solution, the hardware synchronizes data across all drives. Now if a drive fails, the network instantly switches back to running on the remaining drives and sounds an alarm indicating that a drive needs replacing.

A brand new drive can frequently be installed with no network downtime and the RAID software will automatically copy all of the data from the two working drives to the new drive. A failed drive in a network without a RAID solution requires several hours (at least) of work to recover data from backup media.

Agility Networks always recommends a RAID solution for all businesses, since it significantly reduces the risk of network downtime due to disk drive failure. For most companies the benefits far outweigh the costs of implementing a RAID solution.

The final piece of the puzzle is one that most business owners don't even want to think about. Disaster recovery. The whole purpose of making backups and having RAID solutions is to protect against parts of your network failing.

What if the whole network, all of your computers, were destroyed? When most people think of disaster recovery, they think of fires and floods. While natural disasters make the headlines, a network disaster is more likely to come from acts of people, either accidental or deliberate.

- **Your network is more likely to be destroyed by a plumber accidentally turning on the sprinkler system, a pipe bursting in the office above you or theft by a disgruntled employee than a natural disaster.**

While large companies spend millions on disaster recovery plans, small businesses need not break the bank for a disaster recovery plan. The bottom line is that there needs to be a plan. It may not be as detailed or as extensively tested as the plan for a large company, but it needs to be thought out, written down and tested as often as practical.

A disaster recovery plan is like an insurance policy for your business. Any time or budget expended against it may seem like a drag on the bottom line. Right up to the point where you need to use the insurance and then, like many insurance policies, it looks like the best investment ever made.

3. WE HAVE ANTI-VIRUS SOFTWARE ON ALL OF OUR PC's, SO WE'LL NEVER GET A VIRUS, RIGHT?

Not necessarily. If you are depending on each individual user to download and install every update, you are taking a big risk. All it takes is one user to "forget" a couple of updates and you become much more vulnerable to viruses. As with many network security issues, a major source of business risk is human error. Viruses can range from fairly annoying to downright destructive.

- **If just one person on your network gets infected with a truly destructive virus because they "forgot" to update their computer, it can destroy data on your whole network.**

To avoid this risk, Agility recommends virus protection software that is centrally managed such as Symantec's© Norton Anti-Virus Corporate Edition. This software solution allows technical staff to install software on the server and configure the software to "push" software and updates to the client (or desktop) computers.

It significantly reduces the risk of human error as long as it is correctly installed and maintained. Not only does this save extensive time and resources during installation, it also creates a single point of management that makes it easier to check for proper functionality across all devices.

Even further, the properly configured, centrally managed software can adhere to more aggressive and stringent update guidelines. For example, a centrally managed virus protection server can check for new virus definition files every 10 minutes, 365 days per year, without any noticeable effect on the network.

4. SERVERS, PC's AND FIREWALLS NEED TO BE CONSTANTLY AND CORRECTLY UPDATED.

Microsoft makes available three different types of updates for servers and PC's - Service Packs, security updates and patches. Service Packs, which consist of fairly significant feature upgrades, some bug fixes and a hodge-podge of smaller updates; Service Packs are released very infrequently. Security updates are fixes for known network security threats. Security updates are released frequently because they fix network vulnerabilities discovered either in the field or in the quality assurance lab. Patches are usually bug fixes.

However, all software vendors release updates to their software and knowing what to install and when to install it is not as easy as it seems.

To illustrate this point, we'll use an example that appeared on the front page of the Wall Street Journal more than one year ago. When Microsoft released Service Pack 2 for Windows XP, many small businesses dutifully downloaded it and installed it. As soon as they did this, some of their other programs simply stopped working.

What Microsoft had failed to adequately warn people about was that while the Service Pack was available, installing it would disable 20 different programs. The most significant program that it disabled was Peachtree accounting software, a popular small business accounting package used by thousands of companies.

To be fair to Microsoft, it was in the "fine print" but that didn't matter to thousands of small businesses who could no longer use their accounting software.

Microsoft eventually fixed the problems, but their response to the controversy was that it is the responsibility of the organization or individual to read the fine print and decide whether or not to install any update, or any part of an update, that they make available.

The reality is that it requires significant technical experience to decide which updates should be installed and when. This is particularly critical for server and firewall updates. Hackers target improperly updated servers and firewalls.

- **In fact, a very large percentage of servers that are exploited by hackers are improperly updated. Network security is a deadly serious issue and the business risk is well into the unacceptable range.**

Agility Networks recommends that all server, firewall and application updates be managed by a network professional. The entire process should be fully documented and detailed records of the update history for each device on the network should be stored and maintained.

5. WE'VE GOT A NEW WIRELES NETWORK AND IT'S WORKING GREAT.

Is it secured? Securing a wireless network is as easy as setting the security or encryption setting to "ON." However, many companies find that their wireless networks don't function properly when they set it to secure or encrypted mode, so they turn encryption "OFF." This is almost worse than having no firewall.

Anyone with a wireless connection in the vicinity of your network can now access everything on your network. They don't need any tools to break in, the front door is open. They are a user on your network and if you're fortunate, they will not put themselves on your payroll.

- **If you're installing a wireless network and you can't get it to work properly in encrypted mode, either return all the wireless cards or hire a network professional to configure the system to work in encrypted mode.**

REPORT SUMMARY: MANAGE, DON'T REACT.

Throughout this report we've talked about the most common mistakes that we see small and mid-sized companies make with their networks. While we have discussed each issue separately, they are really all pieces of the same puzzle. To effectively manage your network and minimize your business risk, you need to be proactive in addressing vulnerabilities and weaknesses before they cause problems or failures.

- **Again, this is not about technology, it's about making smart business decisions**.

Everyone knows it makes good business sense to change the oil in your car every 3,000 miles rather than waiting for the engine to burn out and buying a new engine. Your network is nothing more than an expensive business tool. Smart business people recognize that performing regular maintenance on that tool is less expensive in the long run than repairing it or replacing it.

Far too many business owners take the view that as long as their network is functioning, they're not going to invest any money into updating, protecting or maintaining their very expensive business tool. As you can see from this report, not only are they not saving money, they are exposing their company to financial and potentially legal risks that no business owner can accept.

About Agility Networks

Agility Networks has been providing network support services to Chicago area businesses for more than 11 years. As one of the largest and most experienced IT consulting firms serving the small business market, Agility Networks has helped hundreds of small and mid-sized companies protect one of their most important business tools, their network. Business owners choose Agility Networks because of their many years of experience in providing both business strategy and technology consulting services. Business owners stay with Agility Networks because of their fanatical dedication to personalized customer service.

Agility manages computer network systems for businesses with between 10 and 200 computers that are located within 25 miles of their nearest office.

Office Locations
Downtown Chicago – 312-932-0508
Schaumburg – 847-517-7900

Free Offer from Agility Networks, Inc.

For qualified companies and organizations, Agility Networks is offering a free ***Agility Information System Audit.*** Agility will review the most critical components of your network and deliver a set of system recommendations to help minimize business risk and protect your network. The ***Agility Information System Audit*** is a **$1,000 value** but is being offered for free of charge for a limited time.

Call the office nearest you today to see if your organization qualifies for this valuable free offer.

Office Locations
Downtown Chicago – 312-932-0508
Schaumburg – 847-517-7900
www.AgilityNetworks.com
