MC Connect

"Insider Tips to Make Your Business Run Faster, Easier, and More Profitably"

3 Critical Elements of a Solid Data Backup Plan

Justin Shelley

I'm sure you've heard the statistics about how likely you are to lose data, how much it will cost to recover it, how long it will take, how much is likely to never be recovered at all, and how many businesses fail after major data loss. But since 96% of all statistics are made up on the spot (including this one), I won't bore you with the numbers. But I can say one thing for certain: it *will* happen. To everyone. I don't care if your data is on a hard drive, a flash drive, the server, a tape drive (yes, they still exist), or in the cloud. I guarantee at some point you will lose data. You simply cannot prevent it. All you can do is prepare for it.

When we interview a prospective client to see if they are a good fit for us, and vice versa, one of the first questions we ask is about their data backup. Do they have one? Is it running? Has it been tested? To these questions, in order, these are the typical responses: yes, I think so, and no. I won't get into the details of what some people consider to be a "data backup" system. But let me just say that in almost all cases, their backup is inadequate. And I have not yet heard *anyone* tell us that they are actually testing their backup. Holy $%@#!

Here's a fun little experiment to try at the office. Turn off all the computers, tablets, smart phones, and servers. Start counting. 1-mississippi, 2-mississippi, 3-mississippi… How far do you think you'll get before heads start exploding? Now let me ask: how important is that data backup? Yes, I know, it's a dumb question.

There are three critical elements you *must* have in place to guarantee a fast, pain-free recovery of your critical IT systems in the event of a data-erasing disaster. But sadly, most businesses we talk to don't have *any* of it in place.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

- Justin Shelley, Master Computing

July 2015

DENTON, TEXAS

Inside This Issue…

When it comes to backing up and protecting your company's critical data, you need to know for certain – without any lingering doubts – that you could recover your files and be back up and running again fast after a natural disaster, server crash, hacker attack or other data-erasing event.

Yet most business owners and administrators don't know for sure if all of their data is being backed up. Even fewer conduct regular test restores to ensure that their backups are actually working, and many don't have a clue what they would do if they suddenly lost their data or ability to access it due to a fire, flood or other disaster. To make matters worse, almost no one keeps records of software licenses and discs that are necessary to restore a corrupt or critically damaged server – so even if they are lucky enough to have all their data, they soon realize that data backup is only one component and doesn't necessarily guarantee a speedy recovery.

OK, enough small talk. Here are the 3 key elements of a solid data backup plan:

1 – Secure, Encrypted Offsite Backup

While we recommend that you have onsite backup, it's absolutely critical to keep an encrypted copy of your data offsite as well. If a fire burns your office to the ground – or a thief breaks in and steals your server and equipment – or a natural disaster floods your office or makes it impossible to access your PCs and server, the onsite backup will be useless to you. And copying your data to a tape drive or other device and carrying it home every night isn't the safest or smartest system either. Data needs to be encrypted to prevent it from falling into the wrong hands – and if you are storing "sensitive" data (like credit card numbers, financial documents, medical records and information or even client e-mail addresses and information) on an unencrypted portable device you may find yourself having a VERY uncomfortable conversation with your clients (and possibly a 5:00 news reporter) about how you exposed their data to an identity thief or hacker.

2 – Data Recovery and Disaster Recovery Plan

A huge mistake many administrators and business owners make is thinking that data backup is the same as disaster recovery – it's not. Many business owners are shocked to find out just how long and painful the process is to get all their data back after a disaster – and that's *if* they have a good, clean copy of their data in the first place (most are surprised to find out they don't). Just having a copy of your data isn't enough; you need to have a plan in place to get everything restored quickly, which is something that tape drives and other physical backup devices don't offer.

3 – Test Restores

After you have a good backup system in place, you need to test it regularly to make sure it works. There's something very wrong if you aren't doing this simple check at least once a month (possibly more for more critical data). If your current IT person or firm is not doing this, you need to fire them immediately. There is simply no excuse.

So there you have it. Everything you ever needed to know about data backup and disaster recovery. Well, not really. I would have to write a small book to fit it all in. Oh wait. I did! You can download a free copy here:

12 Little-Known Facts Every Business Owner Must Know About Data Backup, Security, and Disaster Recovery
http://www.master-computing.com/12facts/

This Month In Technology History

Jay Hathi

We're shooting back 31 years in This Month in Technology to July 1, 1984 - the day that saw the consumer electronics division of Atari Corporation swallowed by Commodore International, best known as makers of the Commodore 64 home computer. It marked the end of an era of dominance in the home and arcade gaming sphere by the company, but it was merely a symptom of a larger problem - earlier that year, the bottom had fallen out of the video game market. Up to that point, it was the worst technology related crisis in history.

Atari was founded as Syzygy Engineering in 1970 by Nolan Bushnell and Ted Dabney, two ex Ampex engineers. They wanted to create a clone of the popular mainframe game Spacewar that could be played by the general public. This led to the development of the first ever arcade game - Computer Space. However, poor distribution and a perception that the game was too convoluted kept the game from achieving mainstream adoption.

In 1972, Syzygy, now renamed Atari to prevent lawsuits from a similarly named roofing company, tried again with a simpler game based on table tennis - Pong. Atari manufactured and distributed the game themselves, and the game was an instant hit. Atari grew exponentially in the years that followed, and became the name in electronic gaming with a slew of successful arcade titles and a string of Pong consoles designed for use at home.

In 1977, Atari released its Video Computer System (later the Atari 2600, after its internal part number). Although it was not the first home video game system to allow the player to change games via cartridge, it quickly became the most popular home game console on the market due to its exclusive content and (for the time) high quality games. Atari was able to license Taito's wildly successful arcade game Space Invaders for the console in 1980, and sales of the 2600 skyrocketed.

By mid-1982, Atari had sold 10 million 2600s and was by and far the leader in home gaming. But at the end of 1982, Atari announced that its growth was coming to a halt - they'd only grown about 10 to 15 percent in Q4 of 1982 as opposed to the fifty percent anticipated by the company. By the end of the year, Warner Communications, the owner of Atari, saw their stock price plummet and their profits cut by 56 percent. The picture grew bleaker as 1983 rolled on - Atari lost $536 million that year, and in September, they famously buried a glut of almost 700,000 unsold games in a New Mexico landfill. What had gone wrong?

In short, Atari's hubris had caused its downfall. The company was notoriously volatile - different divisions of the company considered themselves and their products to be at war with the company's other divisions, and Atari had a reputation among dealers for being incredibly difficult to deal with. In a rush to pump out games as fast as possible, Atari pushed out two high-profile games (Pac-Man and E.T. the Extra Terrestrial) in huge quantities that simply weren't ready to be in the hands of the public. But public tastes were also changing - more and more consumers skipped buying video game consoles or going to the arcade and began playing games on their computers, and new forms of entertainment such as cable TV began vying for the time of consumers.

However, Atari was not the only company that suffered. Other video game makers, particularly Coleco and Mattel Electronics, also found that the video game industry was growing too slowly to fulfill the demand required for them to get rid of the huge stocks of games they'd built up. By mid-1984, Mattel would leave the video game business for good, and in 1985, Coleco stopped manufacturing electronics.

But since Atari was a much larger company than Coleco or Mattel Electronics, and had a more diversified portfolio than either of these companies, it was able to continue operating, albeit at a heavy loss. Rather than try to regroup the company and put it back into profitability, Warner decided to sell Atari in mid-1984 to someone who could. Near the stroke of midnight on July 1, 1984, Warner was able to strike a deal with Jack Tramiel, CEO of Commodore International, to sell Atari's consumer products division for $240 in stock. Warner retained the arcade division of the company, but decided to sell it just one year later to Japanese arcade manufacturer Namco.

However, the buyout by the biggest personal computer manufacturer in the world couldn't stop Atari's slide. After several more attempts at releasing a successful console, the company was sold again in 1996 to hard drive manufacturer JTS, who nearly destroyed the company, before being sold once again to Hasbro Interactive in 1998. Atari is now a wholly owned subsidiary of Infogrames, who mostly use the Atari brand to sell re-releases or remasters of famous titles from the 80s.

“It Never Hurts To Ask”

“It never hurts to ask.”

We often hear that said. But is it true? Recently someone asked me for a favor. The request came in an impersonal e-mail that was obviously sent out to multiple people. I had some business dealings with this person many years ago; however, since then, I had heard from them only once when they asked another favor.

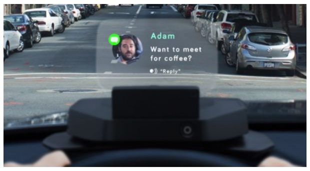
I was being asked to promote something on my social media network. The request did not offer an excerpt, a preview, a sample or any compelling reason why I should offer my assistance and ping the people on my e-mail list.

I thought, “Why should I help?” The implied assumption that I owed this individual something, or that I should help for no reason other than that they asked, seemed a bit off-putting. Have I helped an unfamiliar person before? Yes, there have been circumstances where I was glad to do so. But “Do this for me because our paths crossed” is not a good reason. Sometimes it *does* hurt to ask. Sometimes it comes across as inappropriate or entitled. Asking someone for a favor when you have no relationship with them *is* a bad idea. Naturally, most people like to help — but very few people like to waste their time or energy. And *nobody* likes to feel someone has taken advantage of them.

There’s nothing wrong with asking for a favor or assistance. Just make sure you ask the right person for the right reason in the right way. Otherwise, you might damage your reputation and your relationships.

Mark Sanborn, CSP, CPAE, is president of Sanborn & Associates, Inc., an idea studio dedicated to developing leaders in business and in life. Mark is an international best-selling author and noted authority on leadership, team-building, customer service and change. Mark is the author of 8 books, including the best seller *The Fred Factor: How Passion in Your Work and Life Can Turn the Ordinary into the Extraordinary,* which has sold more than 1.6 million copies internationally. Learn more about Mark at www.marksanborn.com.

Shiny New Gadget Of The Month:



Navdy

Many of us realize how dangerous it is to check e-mail or text messages while we’re driving, but we don’t feel like we can afford to ignore our phone. Brand-new product Navdy to the rescue!

Navdy is a transparent Head-Up Display (HUD) that projects information as if it’s floating six feet in front of you. It’s very similar to what commercial airline pilots use. Navdy works with any car, and with all iPhones and Androids.

Using the apps you already have on your phone, and with no service plans required, Navdy allows you to focus on the road and not on your phone.

As a phone call comes in, Navdy’s built-in camera allows you to simply swipe in midair to answer calls (or dismiss them), so you no longer have to fumble with buttons or touch screens. Plus, Navdy’s voice recognition uses the voice commands you’re already familiar with, whether you use Google Now or Siri.

Any notification on your phone (such as text messages or social media) can be played, read aloud or disabled, based on your preferences. Navdy even allows you to keep your teenagers safe by giving you parental controls.

The product is rumored to retail at $499, but is available now for pre-order for $299. Just visit their web site at: www.navdy.com

7 Secrets To Finding *Relevant* Information Online

Have you ever run into a virtual wall when searching for information on the Internet? With billions of websites online, finding good, relevant information online can sometimes be akin to finding a needle in a haystack.

But take heart! Here are 7 little-known secrets that will help you find what you are looking for in no time at all.

1. Use the "Advanced Search" tool

Almost all search engines have an "advanced search" tool that will provide you with more options for filtering information and websites. This will help you narrow down your search and eliminate irrelevant, off-topic websites.

2. Search with a phrase in quotations

Putting quotations around a phrase will tell the search engine to look for that exact phrase or name instead of each individual word. For example, if you were looking for a chocolate cake recipe, type "chocolate cake recipe" in the search window with the quotes around it. If you left the quotations off, you might get recipes for other cakes or chocolate candy in general because the search engine will look up the words separately: chocolate cake recipe

3. Use synonyms

If your search does not produce the results you want, try synonyms. For example, a dog is also a pet, canine, mutt, pooch, and man's best friend. Use your Microsoft Word thesaurus tool or Merriam-Webster OnLine to find synonyms for your search term.

4. Use a plus or minus sign

This trick will allow you to narrow down a larger category. If you were looking for a roadside café in Atlanta, you would type in "roadside café + Atlanta". This will allow you to search on a specific set of keywords that might not be strung together in one phrase as mentioned in tip #2.

This also works in reverse with a minus sign (-). If you wanted to find all roadside cafes that were NOT in Atlanta, you would type in "roadside café - Atlanta".

5. Just search the domain name

If you know the website you want but can't seem to find the information you are looking for, you can tell the search engine to search for a specific keyword or phrase within that site. Simply enter the search term you are looking for followed by the word "site" and a colon, and then by the domain name.

For example, if you wanted to find information on spam filter updates for Microsoft Outlook, enter this: spam filter update site:www.microsoft.com

6. Eliminate inappropriate content

To eliminate adult sites clogging your search results, simply activate your favorite web browser's adult filter setting. MSN has a SafeSearch option on its settings page and Google's can be found in their advanced search option. It's not 100% accurate but it will eliminate the most obvious sexually explicit websites from your search.

7. Use your search engine's categories

Many search engines offer specialized areas such as news, video, audio, pictures, local, and shopping related categories. If you know you are looking for a picture, choose the appropriate category and your chances of finding what you want increase significantly.

An Urgent Security Warning For Businesses Running Microsoft Server 2003 (And A Limited Free Assessment Offer)

On July 14, 2015, Microsoft is officially retiring Windows Server 2003 and will no longer be offering support, updates or security patches. That means any server with this operating system installed will be completely exposed to serious hacker attacks aimed at taking control of your network, stealing data, crashing your system and inflicting a host of other business-crippling problems you do NOT want to have to deal with.

This is a threat that should not be ignored; if you don't want cybercriminals running rampant in your company's server, you MUST upgrade before that deadline. To assist our clients and friends in this transition, we're offering a **Free Microsoft Risk Assessment And Migration Plan**. At no cost, we'll come to your office and conduct our proprietary 20-Point Risk Assessment — a process that's taken us over 10 years to perfect — to not only determine what specific computers and servers will be affected by this announcement, but also to assess other security, backup and efficiency factors that could be costing you in productivity and hard dollars.

After performing this Assessment for [hundreds] of companies like yours, I'm confident that we will not only be able to expose a number of security risks and issues that you weren't aware of, but also find ways to make your business FAR more efficient and productive. **To request this Free Assessment, call us direct or send us an e-mail today. Due to staff and time limitations, we'll only be able to offer this until the end of July or to the first 10 people who contact us.** *(Sorry, no exceptions.)*

Free Report Download: If You Are Considering Cloud Computing For Your Company—Don't, Until You Read This…

INTRO TO CLOUD COMPUTING

"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud"

Discover What Most IT Consultants Don't Know Or Won't Tell You About Moving Your Company's Network To The Cloud

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report, "**5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud**."

This report discusses in simple, non-technical terms the pros and cons of cloud computing, data security, how to choose a cloud provider, as well as 3 little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated.

Even if you aren't ready to move to the cloud yet, this report will give you the right information and questions to ask when the time comes.

Get Your Free Copy Today: http://www.master-computing.com/cloudreport

The 5 Most Dangerous Pieces Of Information To Give In An E-mail

In the book *Spam Nation*, investigative journalist and cybersecurity expert Brian Krebs revealed the single most effective (and relied upon) way cybercrime rings gain access to your bank account, credit cards and identity. Ready for it? E-mail.

Whether it's opening an attachment infected by a virus, or a phishing scam where you unknowingly give up your login to a critical web site, e-mail still remains the most popular and reliable way digital thieves can rob you blind, steal your identity and wreak havoc on your network. Worst of all? You're INVITING them in! While there are a number of things you need to do to protect yourself, here are five pieces of information you (and your team) should NEVER put in an e-mail.

1. **Your social security number.** Think of this as your "bank account" number with the government. You should never e-mail this to anyone because it can be used to open credit cards and steal your identity.
2. **Banking information.** Your bank account numbers, routing number and online banking login credentials should never be e-mailed. Further, avoid sending a voided, blank check as an attachment to an e-mail.
3. **Your credit and/or debit card information.** Never update a credit card via an e-mail! If you need to update a card with a vendor, there are two safe ways to do this. The first is to log in to your vendor's secured site by going to the URL and logging in. Do not click on a link in an e-mail to go to any web site to update your account password or credit card! Hackers are masters at creating very legit-looking e-mails designed to fool you into logging in to their spoof site, which looks very similar to a trusted web site, to enter your username, password and other financial details, thereby gaining access. Another way to update your account is to simply call the vendor direct.
4. **Login credentials and passwords.** You should never share your passwords or answers to security questions with anyone for any site, period.
5. **Financial documents.** An attachment that includes any of the above is just as dangerous to e-mail as typing it in. Never e-mail any type of financial documents (or scans of documents) to your CPA, financial advisor, bank, etc.

Remember: Banks, credit card companies and the government will never ask you to click a link to provide them with any of the five items above. If you get an e-mail requesting you to update any of the above information, there's a good chance it's a phishing e-mail from a hacker. Don't be fooled!

Vacation Alert!

The ONE Thing You And Your Employees Should NEVER Do When On Vacation

‘Tis the season when you and your team will be taking a little time off to head to the beach or your favorite vacation spot, and while we know we *should* completely disconnect from work, most of us will still check e-mail and do a little work while away — and that could end up causing some issues if you’re not careful while working remote.

So before you head off to have a little fun with your laptop tucked under your arm, keep this in mind: never automatically connect to “any available network.” Not all Internet connections are secure, so if you’re going to log in to the company’s network, e-mail or other critical cloud apps that are hosting sensitive information, only do so on a trusted, secured WiFi and never a public one. We recommend investing in a personal MiFi device that acts as a mobile WiFi hotspot if you’re going to be traveling a lot and accessing company info.

Second, turn off the ability to automatically connect for all of your mobile devices and laptops. You will still be able to connect manually, but it will prevent your laptop or device from connecting to a questionable network without your consent or knowledge.

Finally, disable all printer and file-sharing options on your mobile devices. This is another way hackers can gain access to your network. In an ideal world, you and your employees would take a true break from work, but if they aren’t able to completely detach themselves, then at least require them to stay safe using the above tips.

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winner of last month’s Trivia Challenge Quiz is Nick Blaine from DISD! He was the first person to correctly answer my quiz question from last month: **June was named after the Roman goddess Juno. She was the goddess of what?**

a) marriage and childbirth b) fruit and trees

c) religion d) love and beauty

The correct answer was **a) Marriage and childbirth.**

Now, here’s this month’s trivia question. The winner will receive a gift card to **Chick-Fil-A**!!!

Which kind of animal did Florence Nightingale often carry around in her pocket?

a) Kitten b) Puppy c) Owl d) Snake

E-mail Us Right Now With Your Answer!

Trivia@Master-Computing.com

The Lighter Side:

Great Starting Salary

Fresh out of business school, the young man answered a want ad for an accountant. Now he was being interviewed by a highly agitated, arrogant little man who ran a small business that he had started from scratch.

“I need someone with an accounting degree,” the man said. “But mainly, I’m looking for someone to do my worrying for me.”

“How’s that?” the would-be accountant asked.

“I worry about a lot of things,” the man said. “But I don’t want to have to worry about money. Your job will be to take all the money worries off my back.”

“I see,” the accountant said. “And how much will my position pay?”

“I'll start you at 85,000,” responded the owner decisively.

“Eighty-five thousand dollars!” the accountant exclaimed. “How can such a small business afford a sum like that?”

“That,” the owner said, “is your first worry. Now get to work.”