



**★ EXCLUSIVE ★**  
**THE NEIGHBORHOOD ISSUE**  
*How knowing the local landscape will grow your business*

may + june

**BUSINESS INTELLIGENCE FOR THE CRS PROFESSIONAL**

**2016**

# THE residential SPECIALIST



Council of Residential Specialists  
The Proven Path To Success



**ALSO IN THIS ISSUE**

- ✚ Buying near a **big-box store**
- ✚ How to **protect your data**
- ✚ New rules for **cash purchases**
- ✚ The power of **designation**
- ✚ Check in with a **local chapter**
- ✚ **Team-building tips**





# PLAY IT **safe**

*Data backup and strong encryption software are your best defense against data disasters.*

By Donna Shryer

↘ Data disasters come in all shapes, sizes and disguises. However, there is one constant, according to Bret Piatt, CEO, Jungle Disk, a data-protection service that provides encrypted backups, secure cloud storage and instant file access. "In terms of losing data, it's not if ... but when."

Knowing how and why small-to-medium-size businesses most commonly lose data provides insight into proactive steps CRSs can take to help prevent data losses. With that in mind, a 2015 survey commissioned by Carbonite and conducted by Spiceworks, a professional network for IT professionals, delivers the following statistics:

→ Roughly 65 percent of all reported data losses link to **human error**. This includes accidentally deleting a file, damaging hardware (think spilling coffee on a laptop) and losing

data-loaded devices to theft. Another type of human error overlaps with security incidents and focuses on spear-phishing scams—emails that contain malicious attachments or links. When downloaded or clicked, malware invades the user's computer and cybercriminals gain access to company data. Sometimes online culprits usurp data to steal identities, other times they encrypt company files and demand a hefty ransom to unlock the data. Human error comes into play when links or attachments are hastily clicked or downloaded without confirming that the email is from a trusted sender.

- Next up are **technology failures**, which account for about 29 percent of all lost data episodes. This bucket includes fried hard drives, corrupted applications and outdated software.
- **Security incidents** account for 22 percent of all data losses. These events include viruses,

malware and ransomware. Criminals instigate the disaster, but human error often ignites it, so protective steps to avoid security incidents have to come from multiple angles. The effort is worth it, Piatt says. "Data breaches and hacker attacks may not be the most common reasons for data loss, but this set of scenarios is often the most damaging to your business."

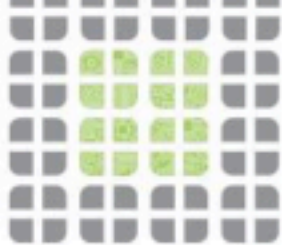
- **Natural disasters**, such as fire, flood, hurricane or tornado, represent another cause of data loss. The unpredictable nature of such incidents, coupled with inadequate reporting, makes it tough to estimate how much data is lost due to natural disaster. However, most experts put this figure at or below 5 percent, which is small, but nonetheless devastating if experienced.

## BY THE NUMBERS

Operating system vulnerabilities accounted for **13%** of all reported computer security issues in 2014. Software vulnerabilities accounted for

**80%**

Source: BeyondTrust



streamlining your business through technology

### 3-2-1

Your best defense against data loss, regardless of cause, is backup, backup and more backup. Among data backup and recovery experts, a commonly

cited backup best practice is the 3-2-1 rule: three copies (the original plus two backups) saved in two different locations (internal hard drive, memory stick, cloud, external hard drive, remote computer, etc.), with one location off-site.

Redundancy is at the root of 3-2-1, so no matter what triggers a data loss, at least one backup should always be available.

### Set Your Sights Off-Site

For Edwin C. O'Malley, CRS, broker/salesperson with Diane Turton, a REALTOR® in the coastal town of Bay Head, New Jersey, saving data to an off-site location is a requirement—a step that saved his and his partner's data after facing the perils of Hurricane Sandy in 2012. "We lost our computer," O'Malley recalls. "But I was backing up to the cloud through Iron Mountain, so once we settled into a temporary office, I downloaded all of our business files onto a new computer."

The cloud isn't your only off-site option, as explained by Eric Baucom, CRS, broker associate with REMAX Gold Coast REALTORS® in Ventura, California. Baucom uses the free version of Code42's CrashPlan. "You can back up data to an internal or external drive and also to any Internet-connected computer. I program backups to my son's computer located across the country in Philadelphia."

### To Pay or Not to Pay

Some data protection services are free and some have a monthly or annual fee. Paid services, according to Piatt, generally have stronger data encryption capabilities,



also #1 in 2014	123456	123456789
also #2 in 2014	password	football
	12345678	1234
	qwerty	1234567
	12345	baseball

To create a nearly uncrackable password, Splashdata offers three tips.

- ➔ Use passwords with at least 12 characters and a mix of character types, such as letters, numbers and symbols.
- ➔ Avoid using the same password over and over.

although the price need not be prohibitive. "You can get started with a service that costs less than \$10 a month and has no annual contract. What's important is that whatever service you choose acts like a safe deposit box. Only people with 'the key' and account credentials can gain permission to view your data."

After being a victim of cyber hacking and experiencing multiple computer crashes, Lilli Rachel Stevens, CRS, Island and Resort Realty in Fort Lauderdale, Florida, does not take chances when it comes to data security. She uses three services to protect her data. She uses Time Machine (available on Macs), which automatically backs up her computer multiple times a day to an external hard drive, and Carbonite, which periodically backs up her computer to the cloud. She also uses Intermedia's SecuriSync, which has file sharing and automatic backup, allowing her to access her files from anywhere. "These definitely aren't

## EASY OPEN

Splashdata, provider of security applications and services, recently announced its 2015 "Worst Passwords List." The 25 winners—or better put, losers—represent the weakest, most-often-guessed passwords by hackers and identity thieves.

Here's the list, starting with the No. 1 worst password.

welcome	dragon	princess
1234567890	master	qwertyuiop
abc123	monkey	solo
111111	letmein	password
1qaz2wsx	login	starwars

- ➔ If tip #2 makes it impossible to remember which password goes with which site, open your favorite browser and search "password manager." Results will include multiple programs that organize, protect and even generate passwords.

the least expensive choices," she states. But if the fee ultimately saves a deal, keeps a client or protects my reputation, then I figure the system has paid for itself tenfold."

John Graff, CRS candidate, a REALTOR® and owner of John Graff Real Estate in Los Angeles, relies on Carbonite to securely back up data to the cloud 24/7. He also talks up his attention to protection. "We highlight our data and cybersecurity to buyers during listing appointments and on our website. It differentiates us in an area that's increasingly important to our clients."

### Public Enemy

While cybercriminals often invade databases through targeted spear-phishing scams, they can also waltz into your database via public Wi-Fi, which is precisely what happened to Cindy Siok, CRS, principal broker with At Home Hawaii Real Estate Sales & Property in Honolulu.

"We suffered a data breach when a co-worker accessed the Internet through a free Wi-Fi hot spot," Siok explains. "So now, when my smartphone or tablet asks if I want to connect to free Wi-Fi, I click 'No' and rely on my personal data plan."

Another way hackers wiggle into your database is through a drive-by download attack, which happens when you visit a compromised website that dumps malware into your computer. Security flaws in your Web browser, operating system or software open the door. The solution, Piatt says, is to protect the network inside your office. "Your router may offer some protection, but today you need additional security from network-level attacks. Because many smaller businesses lack security, hackers are increasingly targeting smaller businesses."

In fact, according to panelists at the Risk Management and License Law Forum, presented during the

2015 REALTORS® Conference & Expo, small real estate businesses, agents and their clients are fast becoming the targets of sophisticated cyber scammers.

To work around cyber disasters, Tom Polk, CRS, real estate broker with Stanberry and Associates REALTORS® in Austin, Texas, recommends Sandboxie, available in both a free and paid version. The program uses isolation technology to block malicious software, viruses and ransomware threats. As Polk says, "Sandboxie allows me to click a link or open a website in a sort of virtual computer. I can see immediately if there's something squirrely going on, and I can close the browser with no harm done."

As for emails with links that seem to be from a trusted sender, but you're not sure, O'Malley suggests this trick: "Hover over the link—without clicking it—and check the URL of the link in the

lower-left corner of the screen. If you see a trusted website, you're probably OK. If you see something suspicious, delete the email."

### The Best Offense Is a Good Defense

For REALTORS®, it's time to get serious about data security. The goal is to find a data-protection plan that fits your budget, suits your needs and makes clients feel safe. As Baucom says, "If you're smart and proactive about protecting your data, then you're free to do what you do best—which is helping clients buy and sell homes." ❖

*Donna Shryer is a freelance writer based in Chicago.*

■ To download the free study Backup and Disaster Recovery: The IT Experience, commissioned by Carbonite and conducted by Spiceworks, visit [carbonite.com](http://carbonite.com), click RESOURCES, and click "white papers." Here you'll find several additional related reports.



## GADGET INSPECTOR

### THE GALAXY S7 EDGE IS A STANDOUT

The new Samsung Galaxy S7 Edge is turning heads in the Android community. Its sleek design and curved edges combine a 5.5-inch display with a narrow grip, making it easier to use than other large smartphones. It features an enhanced camera with dual-pixel technology and 32GB of storage, with the option to add an additional 200GB with a microSD card. Bonus: it's water-resistant.

For more information, visit [samsung.com/us](http://samsung.com/us). Starting at \$750.



### POCKET APP SAVES IT FOR LATER

Pocket allows you to save anything from any device—smartphone, tablet or desktop—for later viewing. It's perfect for collecting articles, blog posts and videos you don't have time to read or watch at the moment, but want to be able to find later. You can save items to "Your List" via email, from your browser or directly from apps, including Facebook, Twitter and Flipboard. A premium option makes "Your List" permanent and easier to organize.

For more information, visit [getpocket.com](http://getpocket.com). Free.



### A SMARTER SMART WATCH: THE GARMIN VIVOACTIVE HR

The Garmin vivoactive® HR is part smart watch, part fitness tracker. It tracks your activity and stats all day with its GPS-enabled built-in sports apps, and smart notifications allow you to stay connected to your iOS and Android devices. It tracks your calories burned, daily steps and sleep, and can now track floors climbed, too. The highlight feature is that it can measure your heart rate from your wrist with the new Elevate™ wrist heart-rate technology. Its water-resistant technology and battery, which can last up to eight days, will also help keep you moving.

For more information, visit [garmin.com](http://garmin.com). Starting at \$250.