eGuide

CREATING A BETTER BACKUP PLAN

GallerySystems
Collect. Manage. Share.

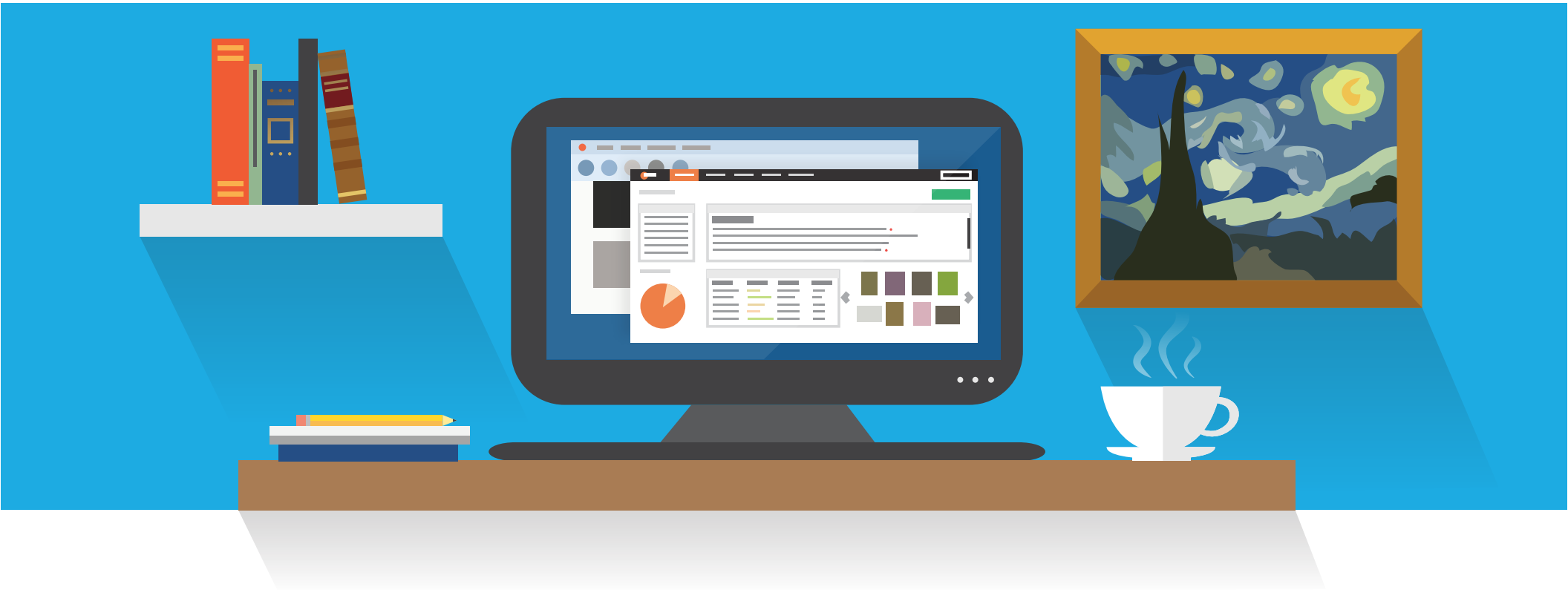
CONTENTS

ABOUT THE AUTHOR: DAVID CUMMINGS

Systems Engineer, David Cummings, is Gallery Systems' network and database administrator and supervises the network security for our clients' data.

With telecom and computer networking experience spanning three decades, David is a Microsoft Certified DBA, a Microsoft Certified Systems Engineer, and a Cisco Certified Network Administrator.

eGuide



BACKING UP IS HARD TO DO

We all know the importance of backing up data. Backups ensure business continuity, support worker productivity, satisfy legal archive requirements, and provide for disaster recovery. But, there are many things to consider in developing and maintaining an enterprise-level backup plan. Accounting for all data needing backup can be a challenge. The purpose of this guide is to suggest ways to ensure your Backup Plan accounts for all necessary data and is as secure as possible.

THE FRONT LINE OF THE BACKUP PLAN

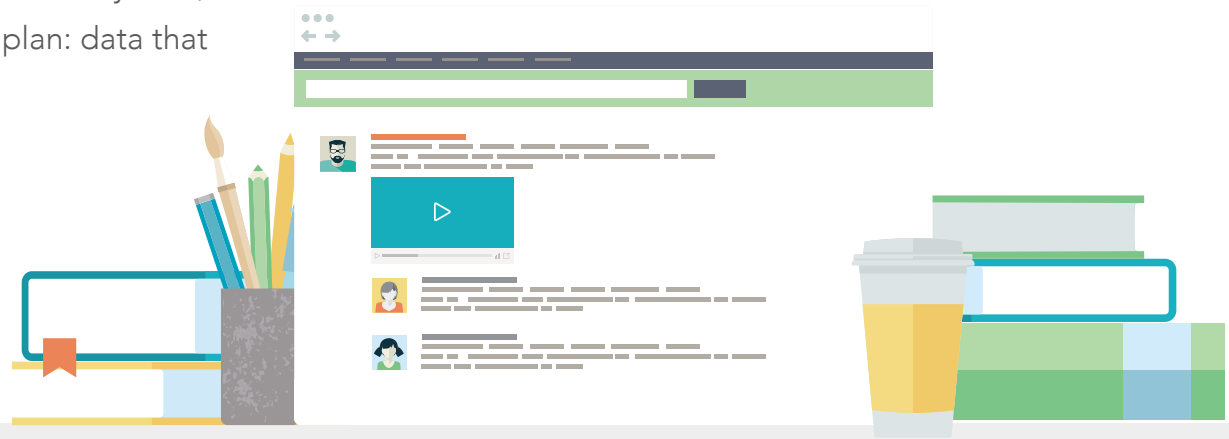
In an old Sex and the City episode, a Mac repair tech asks a distraught Carrie Bradshaw, "When is the last time you backed up your work," and she says, "I don't do that." Later, friend Miranda asks about backups, and Carrie says, "You know, no one talks about backing up. You've never used that expression with me before, but apparently everybody's secretly running home at night and backing up their work."

Times have changed since 2001 when that episode aired, and no one today would be surprised by the question of backups. Of course there are backups. That's what IT does, isn't it? Backs up our work?

The answer, however, is yes and no, because in any organization, office or development environment of any kind, there are going to be holes in the backup plan: data that should be getting backed up simply isn't.

In the case of poor Carrie Bradshaw, her entire laptop (and her life's work as a columnist) fell victim. If her friends had thought to ask the question, "Do you backup?" before her laptop crashed, they would have been performing the task of Front Line Backup Activity: identifying the holes in the backup plan by talking directly with the data contributors themselves.

The Front Line of the Backup Plan is the users themselves; and "users" include IT personnel. In your Backup Plan, everyone should be queried regularly about any possible data that should be backed up but isn't being backed up.



HOLES IN THE BACKUP PLAN

For any enterprise organization, the Backup Plan normally includes backing up things like shared network drives, published UNC folder shares, shared SQL database servers and their databases, shared Oracle database servers and their instances, mail servers and all email and associated data, Domain Controllers and the Active Directory database, media servers and all their stored media, as well as other data objects that might be unique to a particular institution.

But what are some possible holes in the backup plan?

Holes in the backup plan can be grouped by whether they are user-related problems (problems on the Front Line) or more IT-related (problems on the Back End). IT-related holes are problems with servers, software and the organization of backups.

Here's a quick summary of problem sources:

USER-RELATED (FRONT LINE)

a. Work in progress: the data being keyed in at any given moment
b. Local hard drives on user workstations and laptops
c. Servers created by non-IT personnel

IT-RELATED (BACK END)

a. Data waiting to be backed up
b. Online data under attack
c. Backup data accessibility problems

SOLVING THE PROBLEM OF LOCAL WORK

Items 1a and 1b can be considered together. The problem is basically one of protecting the user from losing the work she is performing at any given moment.

Here are some solutions:

1. Encourage users to work directly on networked drives, or in network-shared UNC folders at all times. That way, whenever they hit the save button, they are saving directly to the most robust drives in the organization. Though not always possible due to issues of connectivity or impeded productivity, this should be considered.

2. Encourage users to make use of simple synchronization programs, such as Beyond Compare, that are cheap to buy and easy to use. Then, if they are saving to their local drives, they can periodically synchronize their drive with the associated network path. Users will often balk at doing this, but in the long run may find that the pain of the extra save is outweighed by the gain of never losing their work.

3. Use Microsoft Office products, or other software that have background saves. Google docs is also an option, though there might be security considerations. Encouraging users, whenever possible, to use software that has automatic save capability, prevents or limits lost data when their computer suddenly crashes.

4. Remind users to save regularly. If they are creating content using software that doesn't have auto-save functionality, they should be hitting the save button regularly. We've come a long way from 2001, but it's still all too common for IT personnel to hear the lament, "I was typing all afternoon and my computer crashed and I lost everything."

5. Consider the use of auto-save plugins, of which there are many, to backup work on software that doesn't have auto-save capability.

6. Fortify the Front Line by making sure you know what user data should be backed up, such as local document folders, and that users know to report any new sources of data that should be included in backups.

7. Encourage laptop users to use network shares and/or folder synchronization as much as possible, especially if they are on a laptop that doesn't have a RAID set (which is most laptops).

8. Consider using SSD drives. Laptops represent a special problem because they typically do not have or support two drives, and those that do, don't generally support hardware RAID. SSD drives are perhaps more reliable than HDD drives.

9. Have users work in RAID sets on their local computers, since some computer crashes involve the local disk drive.

10. Consider the use of auto-synchronization programs that run in the background, across the network, synchronizing user document folders with network shared folders. RAID sets can fail, data corruption can be transmitted across all members of the RAID set, and it is possible to have a situation where the data on a workstation drive or drive-set is completely inaccessible. This type of failure can be mitigated by having ongoing auto-synchronization of data between important folders on user workstations and related folders on network shares.

11. Consider using Windows Shadow Copy where applicable, though the pros and cons of this service must be discussed in your organization.

Each user's work represents time. That's time purchased by the organization, and time dedicated to the project. As much as possible, the goal of any backup plan is to avoid having to go back and re-create the work, and re-spend the time.

eGuide

SOLVING THE PROBLEM OF

SERVERS CREATED BY NON-IT PERSONNEL

In many organizations, especially software development organizations, non-IT users have the ability to create their own virtual machines, and build their own database servers. If this is the case, special care must be given to ensure IT is up to date. You want to avoid any situation like this: A distraught user comes to you and says, "I just lost a database in which I spent two months writing stored procedures and I need the backups for that database server". And all you can do is repeat the words of Carrie Bradshaw: **"I don't do that."**

SOLVING THE PROBLEM OF

DATA WAITING TO BE BACKED UP

How safe is the data on those mapped networked drives or networked shared folders, the ones that are so ubiquitous in a modern organization, and are so counted on by users to be a safe place to save files? In an organization with only a single-time-zone and dayshift, the backup tape drives turn on after the lights go out. Then, at some point in the evening or early morning, all the new data on the network is fully backed up to tape. But, it's important to consider that normal system backups are point-in-time backups, and data also needs to be protected during the day, while users are adding content and updating databases. Plus, there is the added challenge for organizations with 24-hour operations.

Here are steps to ensure the integrity of data on the network shares between backup times:

1. Utilize RAIDed hard drives. It's likely that all enterprise-aware organizations use RAIDed drives for their network storage. Discussions of which RAID set is best in which circumstance should be ongoing in your organization. Ask questions like: are you using the right RAID level for each given set of data? And, should you reconsider your overall disk drive RAID strategy? A discussion of pros and cons of the different RAID levels available is also important.

2. Synchronize networked data to a secondary set of network folders, because regardless of the RAID level, entire RAID sets can fail. The data on the network shares themselves should be synchronized to a set of mirrored folders on different servers so that if a live shared folder goes offline, the synchronized copy can quickly be brought online with as little lost data as possible. There are many software solutions for folder synchronization.

SOLVING THE PROBLEM OF

ONLINE DATA UNDER ATTACK

Every organization has a security strategy that includes malware protections at the firewall level, at the server level, and at the workstation level. However, malware still gets through. One of the most insidious forms of malware in existence, and one that can only be truly protected against with good backups, is ransomware. Ransomware encrypts your files with an unbreakable encryption, and then delivers instructions for data recovery that involves paying a fee to the ransomware hacker (who then may or may not give you a decryption key).

Ransomware is often distributed to users via a link or download in an email, so it often gets past malware protection software undetected. Once ransomware starts running on a user's workstation, it encrypts all the files on all the drives that workstation has access to, including all the networked shared drives. In a very short time, your entire network drive system is encrypted and essentially destroyed. The synchronization software will propagate those encrypted files to the secondary backups since the encrypted files will appear as updated files, filling those secondary shares with the same useless files that your primary network drives now contain. The only recovery technique for ransomware encryption is to restore from uninfected backups.

Though no protection against ransomware is 100% effective, here are steps that should be considered:

1. Have as much malware protection in place as possible, at both the firewall level and the server OS level.

2. Put a percentage limit in the synchronization software, so that it will refuse to run if it detects changes over a certain low threshold, say 10%.

3. Have the synchronization software address the secondary shares by their UNC paths. Do not have networked drives mapped to the secondary shares. Most ransomware is only aware of drive letters (local or mapped) and doesn't have access to UNC path shares.

4. Perform backups-to-tape as frequently as possible. Tape backups can't be replaced with ransomware-encrypted data. Once data is backed up to tape, it is truly safe (as long as the tape media itself remains viable). If possible, perform incremental tape backups throughout the day.

5. If possible, shift from network mapped drives altogether, and have users save data to UNC paths instead. This might be impractical for large organizations, but should be considered and discussed.

SOLVING THE PROBLEM OF

ACCESSIBILITY TO BACKED UP DATA

If you need to restore data from an offline backup that exists on a tape or on a backup-to-disk hard drive, how accessible are those backups? If you have a large network, a multitude of users, and a huge amount of new data being backed up each week or month, the number of tapes or hard drives in the backup inventory can become large and unwieldy. Also, finding where a particular piece of data is can become complicated. Most enterprise backup software uses catalogs of one kind or another and these catalogs can require refreshing or rebuilding, which means searching through tapes to find the files you want to restore.

In the case of a full system recovery following a ransomware attack, or major hardware failure, it's probably not difficult to find the most recent full+differential system backups, though the time to restore can be significant. But, if someone is asking for a file that was backed up last month, or last year, the search process can be daunting.

Here are strategies to handle problems involving data accessibility:

1. Invest in a tape library device instead of individual tape units, if such an investment is within your organization's budget.
2. Research which backup software to use, with particular attention paid to the method of cataloging and the accessibility of catalogs, particularly old catalogs, even if the particular backup media itself is not online.
3. Consider replacing (or augmenting) tape backups with backups-to-disk, though the pros and cons of that choice should be thoroughly discussed in your organization.
4. Consider replacing or augmenting tape backups with backups-to-cloud-storage, though again, there is a lot to consider on this subject.

SOLID BACKUP PLANS SAVE TIME AND INCREASE PRODUCTIVITY

Bottom line: backups save time and improve productivity, which translates into saved money. They save the user from having to re-write a document or re-enter data. They save the development company from having to re-develop software. They save the IT department from having to re-build an entire network from scratch.

There are practically no Carrie Bradshaws anymore, as most people understand the importance of good backups. It's filling in all the holes that can be tricky, and worth ongoing discussions within organizations. Analyzing whether you have as complete a backup strategy as possible can potentially save your organization lost data, lost time and lost productivity.

HOSTING SERVICES FROM GALLERY SYSTEMS

Gallery Systems offers scalable hosting services that can manage as much or as little of the IT for your collections management application as you need. With Gallery Systems as your hosting partner, your institution's staff will have secure, web-browsing-enabled access to your data from anywhere. We can handle the nightly backups, schedule service upgrades, monitor database health, and perform all other system administration duties. The data always belongs to you and is accessible only to you and your staff as we rigorously follow your rules for data connectivity and security.

ABOUT GALLERY SYSTEMS

Over 800 clients worldwide trust Gallery Systems with the cataloging and management of their collections. For over 30 years, Gallery Systems' collection management and web publishing software has been the leading choice of the finest cultural institutions, from private collectors and museums, to corporate and government archives and agencies.

Find out how we can help with your collections management and application hosting needs.

Visit us today at www.gallerysystems.com/IT.