AUTODESK UNIVERSITY 2014

BADR CAD: Backup, Archive, and Disaster Recovery for the Design Professional

James Gerth – Stantec

CM5459

Learning Objectives

At the end of this class, you will be able to:

- Develop and deploy a backup strategy that works within your organization
- Test and validate data restoration processes using both on-site and cloud techniques
- Implement a long-term data archival plan that meets the obligations of your industry
- Design a disaster recovery plan to better ensure the security and accessibility of design data and files despite unforeseen disasters

About the Speaker

James Gerth is a senior engineering designer and the CAD manager in Tallahassee, Florida, with Stantec Inc., a global, multidisciplinary AEC (architecture, engineering, and construction) firm headquartered in Edmonton, Alberta, Canada. James began working with AutoCAD software in 1985 and has used Autodesk, Inc., products on PCs, Unix workstations from Sun and DEC, and Apple Inc.'s Macintosh computers. As the corporate CAD discipline leader for an ENR (engineering news-record) Top 25 AEC firm, he worked as an AutoLISP programming language developer, NT domain administrator, Unix systems administrator, and web collaboration administrator. In that role, James designed and deployed CAD-centric networks for project offices in the Republic of Singapore and in the cities of Bangkok, Thailand; Atlanta, Georgia; and Dublin, Ireland. James joined Stantec in 2005, taking on a series of design challenges in the Florida Keys and Panhandle regions. In 2012 Autodesk honored James by naming him an inaugural member of the Autodesk Expert Elite program.

badrcad@cadtag.com

Putting together your backup strategy

What risks do you face, how significant are they to your organization, what is the level of effort and expense that is needed to protect against them? How do you prioritize and design a backup strategy to mitigate against the real dangers to your design information?

Risks

- Information loss
- Undetermined file corruption
- User error / blunder / deletion / 'phat fingers'
- PEBKAC / ID10T errors
- Disk failure – workstation
- Disk Failure – server
- WAN/LAN infrastructure issues
- Malware
  - Ransomware
  - Virus
  - Malverts
  - Botnets
  - Zero-day exploits
- DDOS – victim or perpetrator
- Disgruntled employee
- Ex employee
- Soon-to-be Ex employee
- Passwords
  - unauthorized encryption
  - Home Depot experience
- RIAA/BSA/Other
- Network Intrusion
- Industrial Espionage
- Sabotage
- Political Activism
- Fire, Flood, Lightning
- Earthquake, Tsunami
- Tornado, Hurricane, Blizzard
- Extreme Weather
- Katrina, Sandy, Rita
- Climate change
- Litigation and liability
- IRS, FBI, LEO (Swatting)
- NSA, CIA, FISA
- Zombie Apocalypse

The mechanics of backup technology

3-2-1 Rule

Keep three (3) copies of the design information, in two (2) formats, and one (1) elsewhere.

1. A single copy of critical information is never enough – it's far too easy to lose it. Three copies of the data with one remote is reasonably safe, without spending excessive amounts of time, effort, or money.
2. Having the data stored on a different media type protects against hardware failure, even if one restoration method fails, there's a second way to access the data.
3. Stuff happens, and sometimes the only safe place is elsewhere.

One typical approach to meeting that rule would be to duplicate the current version of the digital data files onto a NAS (Network Attached Storage) device, run a daily tape backup, and rotate tapes between in-house and off-site.

What do you need to back up?

Start with presuming that the basics of hardware protection are being addressed, e.g. RAID disk storage, redundant power supply on the servers, UPS and surge protection on all devices. Protecting the operating equipment is step one.

After that, decide what it isyou need to backup. The more data you want to protect, the greater the capacity and expenditures required.

Disk Imaging is a complete backup of everything on a disk. Generally speaking, a disk image can take just as much space as a backup as the disk being backed up uses. For a network server, it's likely that the machine has been configured with a system drive separate from the server data store. Each of those stores can be imaged separately.

Workstations are usually configured with a single disk, with the operating system, documents library, and project data all on a single logical C: drive. From an imaging perspective, that's not ideal. It's better to image separate partitions for the operating system and data/documents, as the OS partition does not need to change frequently, but the Documents folders and project data folders and files on the workstation are changing constantly.

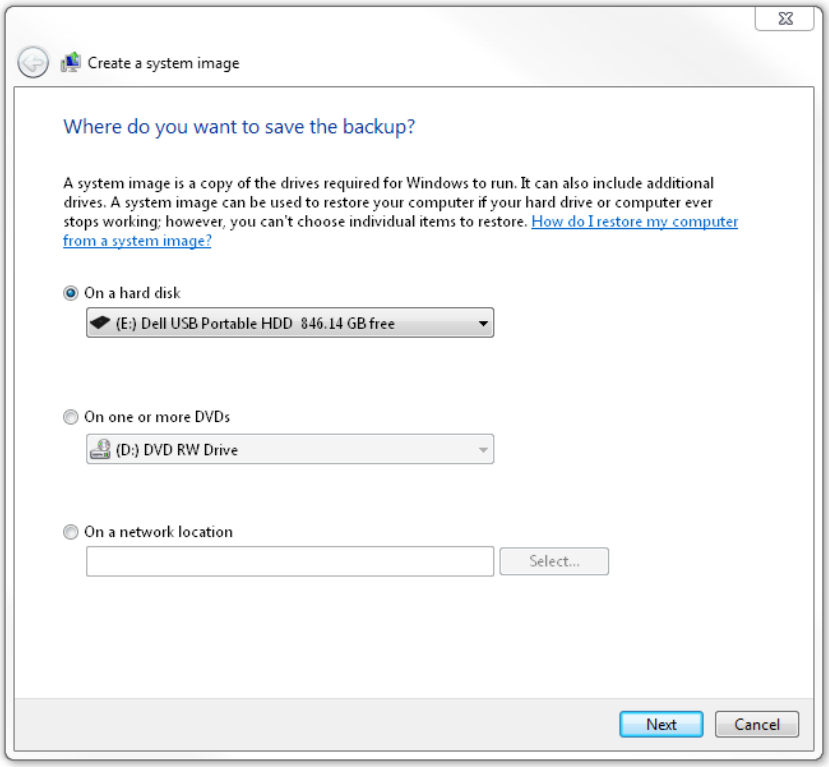
With current disk imaging software, you can create a disk image in multiple ways:

- Another physical disk stored off-line
- A network share that is normally unmounted
- A NAS dedicated for disk images
- Tape

Tools of the imaging trade:

There are both physical and software tool that you canuse. One that I find very handy is a USB/eSATA Hard Drive Dock. This makes it extremely simple to plug in an additional hard drive, and with either USB 3 or eSATA connections, transfer time is pretty reasonable. If you are limited to having only USB 2, then creating a system image of a working drive is going to take a while

For software tools, Windows 7 includes a disk imaging tool, located under Control Panel | Backup and Restore. While frill-free, it is functional.



Additionally, Clonezilla is a very powerful and capable FOSS application for creating disk images. Since it boots into a Linux interface from a LiveCD or USB drive, it's extremely powerful and flexible. The price is right, there's an active development effort on-going, there is an unavoidable learning curve. Being able to boot off of a CD and restore a crashed machine from a zip file on the network is very valuable and a feature worth learning.

And finally there are a number of commercial vendors in the disk imaging space. Many of them combine disk imaging with backup capabilities in suites of applications. With the relatively low price of hard drives, I find it reasonably easy to maintain a spare system disk, and just swap out the drives if there are problems, either physical failures or malware that crept in. Since the OS System disk changes infrequently, bi-monthly or quarterly updates of the system image are adequate.

A larger organization will need to handle imaging and OS refreshes somewhat differently – especially if there is a standard set of licensed software that everyone in the company must have installed. Typically at that scale there's an IT group that manages licensing and will be tasked with keeping the OS functional and patched.

Data Backups

For normal day to day operations, you are primarily concerned with backing up the design data rather than the operating system and applications. Exactly how you handle that will depend to a great deal on the available infrastructure, and how you currently enable access to the design files.

Workstations

If design data is managed and edited directly on the workstations, then your options are limited to generating backups of each machine's data files. This can be done with portable drives, but is rather unwieldy at scales greater than one. (And unwieldy backups don't get done.)

A better choice in this scenario would be to run backups to a NAS (Network Attached Storage) that can be shared by multiple users. Each workstation should have its own location on the NAS drive to backup to.

A third option would be to back up the workstation data files to a central server and then back up the server on a regular basis.

Server

A more efficient scenario is to maintain all your design information on a network server. That offers you the simplicity of a single location to backup design data from. Again, this could be backed up routinely to a NAS, or a tape drive or multi-tape magazine.

The Data Itself

Regardless of the machine you are backing up, you need to determine what design data on that machine needs to be backed up, and when it needs to be backed up. There's little point in backing up .bak files for example, and there's a cost associated with backing up information. A cost in the time required, and the cost of the backup media. The more redundant information you replicate, the longer it will take to accomplish, and the larger the capacity of the data store you'll need.

It critical to maintain in your backups everything you'll need to recover a project or design. That will include the drawings, models, spreadsheets, specifications, documents, correspondence, etc. In an ideal scenario, your folder structure is set up to mimic the work your organization does, so that you can perform backups on a folder by folder basis and save everything you would need to continue working on that job.

Files are relatively simple to backup to a backup data store. That's a simple copy operation. It's much more challengin when there is a live database running, such as Microsoft SQL Server,

MySql, especially with a Document Management System, e.g. Vault or Synergis Adept. If thedatabase is running as a service, it's always live. You'll need to work with the tools provided by the database vendor to make a snapshot backup of the database.

Vertical applications including Plant3d, Map3D, Civil3d may be utilizing Vault or other database connections, and if that's the case in your operation, you'll need to account for that as you set up your backup methods.

Revit is rather more involved, especially if you are running Revit Server as the central repository. If you are managing a Revit installation, refer to the documentation for that application.

The resource or library information is less critical. On my network, we've set up shares that are dedicated to resources used on many different job; specifications, details, client requirements, and so on. It's important information, and needed on all of our projects, but the library content does not change frequently.

Some information really does not need to be backed up. It's either transient, irrelevant, or otherwise not needed. As an example, a server may have a Public or Common shared folder that's used as a dumping ground or transfer spot between several office locations. The intent of those network shares is a temporary spot to park digital data until it can be moved appropriately. Another example could be a 'scan to network' share. Everything pertinent to a project or task should be moved to its proper home, instead of building up endlessly on the server.

The Backup Data Store, aka Cold Storage

There are several reasonable options for keeping the backup data store, and the one you choose will depend on the amount of data you are backing up, and the frequency of those backups. One important consideration is that users, including server administrators, should not have regular write access to the data store. The backup store should always be directly inaccessible. Since malware of various kinds, including ransomware, is a growing threat to your data you need to protect the data from alteration after it has been backed up.

With a workstation to portable disk strategy, the solution is to unplug the backup drive except when actively backing up or retrieving files. On a workstation to NAS backup, the NAS should only be mounted for those purposes. Alternatively you could restrict permissions to the NAS to a specific account, and run the backups from that login context. That would permit you to keep the backup store readable by the normal users, but not writable.

If you are implementing a workstation to server file backup, the preferred approach is to run that from the server, with a Backup Operator account on the server accessing the workstations after hours and backing up the design information from remote access. User accounts can be permitted read privileges, but should never have write access to the backup data store.

Likewise, backing up the server should be done only with a specific Backup Operator account login. Most, if not all, commercial backup software can meet that restriction without problems.

The traditional option for a server backup is tape. This is a well tested, tried, and reliable choice. Readily available tape drives from Dell and other vendors have capacities in the hundreds of gigabytes, reaching up to 3 Terabytes for the Ultrium 5. Sony has announced a 185 Terabyte tape cassette, so the capacity is there, and increasing. At a price of $60 (US) for a single LTO5 tape, you get a lot of available storage. And using a tape loader means you can easily reach 20 Terabytes of backed up data. Tapes do wear out eventually, but are easily replaced with fresh media.

A second choice would be a NAS backup. Essentially a headless computer with network connections, massive storage, a minimalist operating system (typically a Linux variant with SAMBA) and a Web management interface, an office scale NAS is relatively easy to set up and use as a backup. Configuring a 5-bay Ethernet connected NAS with 4 Terabyte drives in a RAID setup permits 16 Terabytes of backup storage.

This type of device can be rack mounted alongside the server, or free standing with nothing but power and network connections. It's even possible to keep the NAS in a separate location, and run backups over your Wide Area Network (WAN) connection. If you've got two or more office locations, it's very do-able to back up Office A to Office B, Office B to Office C, and Office C to Office A. The practicality of that will depend on the bandwith of your inter-office connections and the amount of data you need to transfer over them

Finally, there's the option of Cloud storage. Backing up design information to a Cloud provider possesses the salient virtue of keeping the data 'elsewhere'. And since the vendors are using multiple data centers, it's almost impossible for them to actually lose your information. For that matter, it's almost impossible to actually delete the information you want to delete.

As the owner of the data, you have no control over what happens to it when it's parked with a Cloud provider. As a rule, the data will be encrypted during transmission to the provider, but often once there it's stored unencrypted as plain data. It's accessible to anyone who can physically access it on the other end(s), and you are trusting them to maintain, protect, and preserve the information that is critical to your business.

Tape and NAS are essentially fixed costs. You can decide ahead of time what you will need, and how much to spend, and once you buy the hardware and media, it's yours. Cloud based backups, however, are floating costs. You're paying the vendor for storage capacity, and those prices can change over time. You're also paying for internet connectivity and are subject to price changes there, as well as the likelihood of a backhoe tearing through a cable or fiber optic line between your shop and the vendor.

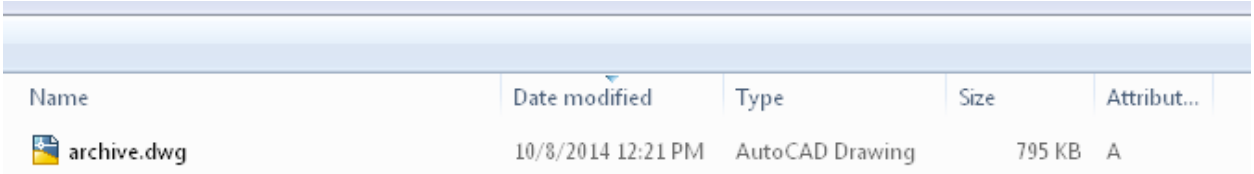
But having critical project information safely stored and secure from physical problems at your physical location can be priceless.

Backup Strategies

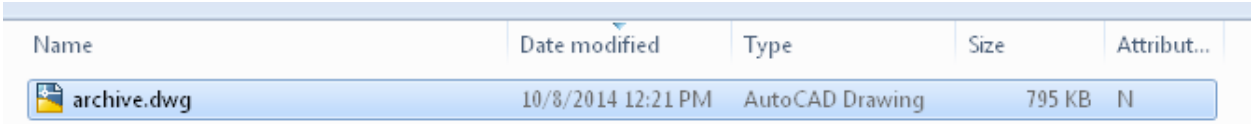
Backups, dollars and data security are related. The more data you want to keep safely backed up, the greater the expense you'll incur. Developing the backup strategy that's right for your organization is going to balance what you are willing to spend against what you are willing to risk losing, along with a realistic assessment of what the risks are in your situation.

First of all, let's want to distinguish full backups from incremental backups. A full backup will gather every file on the drive that matches your backup pattern. An incremental backup will go through that same pattern-matching approach, but only backup files that have been modified since they were last backed up. These two types of backups work together to maximize the amount of protected design information, while minimizing the total size of the backup store required.

Each time a file is edited, created, modified, or copied, Windows sets the **A**rchive bit in the file attributes. An incremental backup will utilize the same pattern matching as the full backup, but will only copy those files that have the archive bit set.



Once a file has been backed up, the backup software or script should drop the archive bit.



Backup strategies are based on doing periodic full backups at a predetermined frequency, followed by incremental backups at more frequent intervals. If the data restoration needed is for a single file, then the most recent incremental backup that has the file on it is the only place you'll need to look. If the file has been modified many times, you can retrieve earlier version from older incrementals.

In a worst case scenario for your data, you can restore a full backup to a bare data disk, followed by incrementals in sequential order. That will give you a complete restoration of the drive as of the last backup.

The combination of a full backup and subsequent incremental backups is referred to as a backup set

Managing Backup Sets

It's usually more economical, if less convenient, to maintain multiple backup sets on tape. While it is certainly possible to implement similar techniques with NAS or spare hard drives, the cost of hardware will be much higher, and more expensive to extend.

There are several well-known ways to manage your backup sets, First In First Out, Round Robin, Grandfather Father Son Towers of Hanoi,. For convenience, I'm going to talk in terms of a weekly backup set strategy and a five day work week, but the time increment from full backup to full backup should be balanced by your hardware infrastructure and budget.

First In First Out

aka FIFO, is probably the simplest method, and can be implemented with only two backup sets. In principle, the initial full backup is run prior to the start of the week – generally over the weekend. The next four business days incremental backups are run. At the end of the cycle, the used backup media is taken off-site, and the next set is brought in to repeat. Each set of tapes/disks is recycled continuously, so there is at most an ability to retrieve data no further back than the oldest complete set.

Round Robin/ Grandfather Father Son

This is basically similar in concept to FIFO, but extends the number of sets, and takes one set off-line at specified intervals. A common approach is to have four or five backup sets, and send the last set out to storage for a longer period of time. Presuming a monthly Round Robin schedule, for week one, backup set one is used, for week two, backup set two, and the same for week three. If week four is the last week in the month, a monthly backup set is used, otherwise the week four set is used and the monthly set is run the following week.

Monthly sets are sent off-site and retained for a longer period of time (three to six months) before being returned to the cycle. Frequently in larger organization the final backup set for the year is retained in long term storage and not reused.

This approach enables recovering any data from the past month from the weekly backups, and older data from the saved full backup going back several months.

A variation that minimizes tape usage would be to continually recycle the four incremental every week, and only change the full backup tapes.

Towers of Hanoi

The name Towers of Hanoi is taken from a well known mathematical game of the same name. In that game, there are three posts, with rings of decreasing size on the first post, and the other posts are empty. The object is to move all the rings from the first post to the third, moving one at a time, while never placing a large ring above a smaller ring.

This is a complex backup strategy, using a recursive method to optimize the backup strategy, minimize the number of tape/disks used while maximizing the length of time the oldest backuo remains available for restoration.

A set of *n* tapes (or other media) will allow backups for 2^{n-1} days before the last set is recycled. So, three tapes will give four days' worth of backups and on the fifth day *Set C* will be overwritten; four tapes will give eight days, and *Set D* is overwritten on the ninth day; five tapes will give 16 days, etc. Files can be restored from 1, 2, 4, 8, 16, ..., 2^{n-1} days ago.[2]

The following tables show which tapes are used on which days of various cycles. A disadvantage of the method is that half the backups are overwritten after only two days.

Three-tape Hanoi schedule

	Day of the Cycle							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Set	A		A		A		A	
		B				B		
				C				C

Four-tape Hanoi schedule

	Day of the Cycle															
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Set	A		A		A		A		A		A		A		A	
		B				B				B				B		
				C								C				
								D								D

Tables Courtesy Wikipedia, Creative Commons Attribution – Share Alike CCL

If you decide to use this strategy, it is strongly advised to select backup software that can implement this strategy.

Backup software

While it's certainly possible to 'roll your own' backup scripts, there are a large number or resources currently available, from GPL PERL scripts, to commercial software. There are considerations that should be kept in mind when choosing what software you will use to implement your backup strategy.

Reliability and compatibility with your equipment is the first priority. If you are going to use an 8-tape vault, then a basic batch file is not going to handle it.

Second is reliability and support. If the software cannot be set up to run unattended and implement the strategy you've chosen without intervention, or there's no ready way to get questions answered and support with problems, then it will not work very well for your setup.

Third is ease of use and flexibility. You want to be able to manage the backup and restoration process without spending large amounts of time tweaking the software to meet your needs. And, since those needs will change, there should be a straightforward, well documented way to change the software configuration as your requirements change.

If you have a live database, look for software that can automate the process of stopping the database server, creating database snapshots, and backing them up. While that can generally be done manually with the database management tools, a backup that's not easy to run doesn't get run.

Finally, a critical, often overlooked factor is logging and notification. There will inevitably be files that fail to backup or validate for one reason or another. You will need to know which ones, and evaluate the problems that caused the backup failure on those files.

A secondary advantage to logging is tracking the amount of changed data. If suddenly your incremental daily backups jump in size while the workload hasn't; that's a cautionary flag that your system may be affected by ransomware or other malware.

Restoring and Testing

A backup that can't be restored is not a backup. The only way to verify the integrity of the backup process is to restore the data and verify that it's correct and intact. Set up a schedule in your calendar, and periodically restore and test the recovered files.

Special Circumstances

At some point, you will encounter a situation that requires deviating from or drastically modifying your backup process. One such situation is the notification if a Legal Hold. This would generally be triggered by official notification of litigation that involves your organization, or by becoming aware that litigation is a real possibility. If a legal hold is mandated, all backup data must be retained, and deletion or recycling of backup media will not be permitted. If in doubt, consult competent legal counsel in your jurisdiction.

Archives

Rule one. Archives are not backups, and backups are not archives.

A backup is a short term mechanism for recovering data from a temporary store. Archiving is a much longer term, and depending on your industry, could range from decades to perpetuity. Every industry and field of practice has separate data retention requirement. Your organization should have a documented data retention policy that has been vetted and approved by management with the advice of legal counsel. If you do not have one, getting one in place should be a priority.

Generally speaking 'archival grade' media should be capable of surviving a century under storage conditions. That excludes a box of random tapes stuffed into a closet, a case of Zip disks, or a stack of re-writable CDs on the shelf. Magnetic media has a limited shelf life – the EM field strength of fluorescent lights will gradually randomize the bit pattern on the media. CD-RW media is based on chemical changes that have been designed to be unstable. CD-R and DVD-R are a little better, but there are still severe limitations on the life of the media, especially under less-than-ideal conditions.

The other concern with using typical digital media is the constant change in technology, media, drives, and formats. After all, even if that box of 5-1/4" floppy disks with the Disney Land site plans was still good, who still has a drive in their office that can read them in 2014? Similarly, decades old magnetic tapes from the last century are unlikely to mate up with the current tape drives. A CD-R of that era will still have a readable disk format, but it's quite likely that the disk itself has deteriorated too badly to read completely. I'm finding that to be too common with four year old CD-R disks.

Contrast that with older methods of recording information. We can read three thousand year old hieroglyphs on the wall of Egyptian temples, Elizabethan manuscripts from the 1560's, or the Book of Kells from 800 CE.

Up until recently, there have been only two real choices for archiving design drawings. The first is ink on mylar. With chemically stable ink, and storage in controlled environments, a usable lifespan of centuries is possible. The second is microfiche. Archival microfiche has been rated for a usable lifespan of a century. Neither one is really suitable for digital data.

For digital media, the only real way to get past the technology changes has been to migrate the data to a newer storage media. Before you throw out that Iomega Zip drive or Sony 40Mb tape drive, transfer everything you need to keep from the old media onto CD-R. And plan on doing it again in three or four years. Bear in in mind that each transfer will accumulate errors, eventually becoming unreadable.

Today there are a handful of vendors producing archival CD-R and DVD-R. JVS is one vendor that can supply CD-R, DVD-R, and BlueRay-R media rated for a 30 year life expectancy. That is under optimal storage conditions, and generally can only be achieved with recorders that are certified by the manufacturer. Once written, the archival CD-R and DVD-R should be readable by typical CD/DVD readers.

There is one vendor, MDisc, that rates their media at 1000 years. They offer both DVD storage at 4.7 Gb capacity, or Blu-ray storage at 25 Gb. ISO/IEC 10995 testing showed the median expectancy of the MDisc DVD-R to be over the millennium mark, at 1,332 years.

Again, while the disc should be readable by any standard DVD or Blu-ray drive, you will need a recorder certified by MDisc as compatible.

One advantage to DVD and Blu-ray long term storage of data is the well documented file system used by those media. While the file formats used by applications change and are frequently treated as proprietary information by the vendors, the standardization of file systems means that the data will be recoverable. You may not be able to open it for editing of viewing if the vendor is gone or has abandoned the editing software, but at least the data itself will remain intact.

Managing Your Archives

The traditional method in AEC firms for locating older project data has been to look for the grayest head of hair in the drafting room, and ask where it is. With the demise of flat files and the transition to digital data, that no longer works. IT may have swapped out servers and re-pathed everything between the date the project was worked on, and the time the data is needed again. Mergers and acquisitions, combined with a mobile work force, are creating a condition of Organizational Alzheimer's, where the memory of what projects were worked and by whom, has vanished with staff and management turnover.

On a short term basis, as CAD managers, we need to take charge of protecting that collective memory. When my prior firm was acquired, the new IT department wanted to sweep everything with a new broom. Their approach to keeping older project data was to copy everything on the old server's project folders to a single virtual drive at corporate headquarters. And while they maintained organization of that data, that organization was lacking in context. There was no metadata. What had been stored and searchable in a document management system is now a vast number of folders of exported documents, dropped in arbitrarily named folders under an obsolete, un-researchable project identification number. The documents, spreadsheets, design information, and drawings are all there, but locating anything of value became an archeological exercise in hunting data.

At my office, we had already taken some initial steps towards archiving project data off the server and putting it onto CDs and DVDs. While I had started this prior to the acquisition of the company, that effort was rapidly accelerated as we transitioned to the new regime. The old scheme has project related information scattered across multiple network drives and a separate

document management system. To place that onto a single disc required exporting from the DMS and copying data from the multiple locations into a single project repository and then burning that to disk. By itself, that would have been an exercise in futility, as locating anything when it was needed later on would have been difficult. The solution we implemented was using a database application designed to catalog CD content. While not ideal, this did allow searching a single database of the content of hundreds of CDs and DVDs.

We selected SmartCD Catalog; www.smartcdcatalog.com, but there are other applications that perform similarly. The ability to add metadata, that is, data about the data was one of the important factors in our selection. We could use that to add comments and notes to the project data for searching, such as the project engineer's name, or the client, location data for the project, or other relevant information. The data is a file, stored as an Access database on our network, and backed up as part of our regular backup processes.

What this particular application does not include is an index of the contents of the files, nor does it automatically include document properties or thumbnail images. These would be helpful features, and are included with the WinCatalog 2014 commercial application. For serious developers, there is the CDCAT application on SourceForge, which currently has no maintainer and has been dropped by the developer. Since it is a GPL licensed application, it's possible to extend and customize the source code to be a better fit for project and design data rather than the music collector. The WinCatalog software uses SQLite for its datastore, while CDCAT relies on an XML file datastore. Non-proprietary datastores are preferred, since there's no certainty than any software vendor will be around or relevant in five years.

Managing For The Long Term

Long term archive management requires a different mindset than is commonly found in either the IT or CAD disciplines. Essentially it calls for the implementation of library science. If your organization maintains a company library with professional staff, you are fortunate indeed. If not, this provides an opportunity to set one up.

The technology behind library catalogs is much more advanced than the relatively simplistic CD Cataloging software mentioned already. With a larger base of potential users, and a large variety in both scale scope of the libraries, there continues to be active development of a number of applications, both proprietary and FOSS (Free and Open Source Software) available. Open source in particular is appropriate for long term cataloging of archived design information, since the public availability of the source code and the open database formats ensures that the metadata and organization of the catalog. Two FOSS Integrated Library Systems (ILS) are well regarded and are in active development, Koha and Evergreen.

Koha, www.koha-community.org, has been in active development since 1999, and is used internationally. Implementations of Koha include the Vermont Organization of Koha automated Libraries, the Spanish Ministry of Culture, and others. There are connectors built with the Drupal Content Management System (CMS) to directly access the Koha catalog from a Drupal site.

Evergreen, http://evergreen-ils.org, was originally developed by the Georgia Public Library system, and is currently implemented widely in the US and Canada. The servers providing the PostgreSQL backend database are running Linux, but the user interface can run on Windows, Apple, or Linux computers, as well as a publicly accessible interface via a web browser.

Document Retention Policies.

As you implement a long term archive, you will need to be keep in mindthe legal requirements for document retention in your industry. There is material you must retain, and material that you can eliminate. Which is which, and how long any class of material must be retained is based on legal requirements. This is an area that you must coordinate with your corporate counsel, and adhere strictly to a company document retention policy, if one exists. If one does not, it's an excellent opportunity to get one developed and implemented.

Physical Storage

While having archived material is god, how you keep it, and where you keep it is important. The archives must be readily accessible, and concurrently protected from any damage or degradation. This essentially means that you need at least three copies of all the media you are archiving. One set should remain on-site, where it and be reached on an as-needed basis. A second copy should be kept in off-site storage, whether with a professional document storage company or a climate controlled storage unit. The third copy must be kept in the most secure location you can justify. As the media is upgraded, the redundant copies off-site and in secure storage need to be replaced as well. It's probably a reasonable idea to include a device capable of reading whatever media you are storing off site. Since that is long term storage, you want to be certain that it will be possible to read that information down the road, regardless of what happens to you primary facility and equipment. One thing you do not want to face a decade or two later is trying to access data from media that readers no longer exist for. Try locating a working Bernoulli drive, or an 8" Tectronix floppy disk reader today, and extrapolate that to 2035 CE.

The Iron Mountain storage facility at Boyers, PA is located 220 feet underground in a former limestone mine. The Hutchinson Salt mine, Underground Vaults & Storage, is located 650 feet underneath Kansas. While not readily accessible, the information you store at these or competitor facilities is protected and safe from harm short of an extinction level asteroid impact.

Distaster Recovery, Road – Meet Rubber

Now that our backup plans are set, the backups are running reliably and consistently, and all the significant historical design information we need to retain is securely archived, cataloged, and stored in safe locations, we can plan for the worst, and decide how to thrive in the recovery period. Whether you call it disaster recovery or business continuity, it's all part of designing a sustainable and resilient organization that can take the bumps in the road and continue on

With the history of disasters since the middle of the last century, a lot of effort has been put into creating resources for disaster recovery. If this is part of your role in your organization, then you need to delve deeply into those resources.

The Disaster Recovery Journal, www.drj.com, publishes quarterly editions of their business continuity publication, which is well worth the subscription. In addition, the website offer white papers on specific topics and case studies.

Ready.gov is part of the *Ready* national Public Service Advertising campaign. This program includes personal and family preparedness information as well as business resources for pre-disaster planning and disaster recovery.

Risk Assessment

The first step is to realistically asses the disaster potential of your locations. Whether it's another Hurricane Katrina, Superstorm Sandy, tsunami, avalanche, Chernobyl type event, dam collapse, building fire, or the New Madrid fault reawakening, every location is at risk from predictable sources. Evaluating what it possible, and what is probable is important in establishing your disaster plan. While tsunamis are unlikely to have a substantial impact on Memphis, the New Madrid fault has the potential to level the downtown area of that city. When evaluating the risks, keep an eye out for industrial facilities that are potential disaster sites, fertilizer plants, railroad lines, chemical processing plants, and so on. And look at the larger area as well – Nashville, TN is 150 miles from Lake Cumberland, but a dam failure there would flood Nashville within a matter of hours.

Unpredictable disasters should be evaluated for risk factors as well, although the very nature of such risks makes planning for them imprecise. The problem of looking down that particular rabbit hole is that the cost of mitigating for the improbable can be prohibitive, and divert resources from the more likely scenarios you will encounter.

Once you have assessed the risks, decide what is feasible to mitigate the impacts of the specific risks. If the building lacks a sprinkler system, explore the costs of installing one to mitigate fire damage. If the location is susceptible to storm flooding, determine what options are available to minimize water damage. Feel free to bring in a fresh set of eyes, such as meeting with the local fire department and your insurer, and listen to what they have to tell you.

Business Impact Analysis

Based on the disaster scenarios you've determined to be realistic, you should develop a business impact analysis. It's worthwhile to examine the impact on your business of multiple situations and understand what the different effects would be from various situations. Contrast for example, a building fire that destroys a single office, a major flood that impacts an entire city, for the small organization with a single registered professional' what if that person was involved in a fatal accident or was unable to work for several months?

Your impact analysis should look at the financial impacts as well as the direct impact on business operations. Consider lost or delayed sales and income, destroyed equipment, inability to deliver design drawings, fines, additional recovery expenses, contractual default, client dissatisfaction and defection, and the inability to implement proposed business plans or expansion that had been in the pipeline.

You will want the analysis to separate the organization's functions into critical and non-critical categories. Critical functions are those that are essential and cannot be disrupted or eliminated, or are required by statute. Non-critical functions are those that can be delayed or deferred without irreparable harm to the organization. With the categorization laid out, you can determine how to assign priorities for continuity.

Business Continuity Plan

With your impact analysis in hand, it's time to gather the stakeholders and work up a continuity plan for the organization.

Planning should be based on the most serious and disruptive possibilities. When a disaster happens, it is more efficient to have a comprehensive plan that takes into account extreme scenarios that aren't needed, than to have a partial plan that has to be expanded on the fly under less than ideal conditions.

The plan should contain contact information; alternate phone numbers and email addresses for critical personnel, including IT staff, senior management, and registered professionals. Also, add contact information for other parties who are involved in your business operations, such as your attorneys, accountants, etc. Senior management should maintain their own contact of important clients and customers off-site, so they can be contacted before the news hits the airwaves.

Since it's probable that the normal business location will be unavailable, plan in, and have a secondary location in mind. At a minimum, establish a meeting point that everyone in the organization knows about as an evacuation spot for fire or other localized scenarios. Make sure that everyone in the organization knows to meet up at that location.

Planning in advance for a second shop to work out of will minimize the disruption, at least somewhat better than not planning will. If you have multiple offices in separate geographic locations, develop a strategy for transferring active jobs to the other sites.

The continuity plan should pay particular attention to safeguarding your design data, documenting how and where off-site backups are stored, who has access, along with any passwords, codes, or keys needed to access them. If you are running network licensed software, develop a strategy for getting that running again if the network servers are down indefinitely, or destroyed completely. Do not forget to build in anti-virus protection during the recovery phase – you'll be more vulnerable than normal, and lacking your normal infrastructure.

As you consider your work processes, and think about how to adapt them to extreme situations, make sure that you actually have them documented, and that those documents are available whenever needed. If you've prepared checklists of tasks to restore critical business functions, test them and assure the stakeholders that the lists and steps are accurate and adequate. As systems and processes change, keep the plan and hardware inventory updated. You should establish projected time frames for recovery depending of course, on the scope of the disaster and the amount of damage that needs to be dealt with. Will there be adequate staff to accomplish the goals in that time?

Some disasters provide warning – and you'll be able to fine-tune your response as the danger approaches. Others will happen almost instantly, and your plan has to detail the responses you need to take. Don't expect to get it right the first time. Test the plan repeatedly. Look for the holes and the elements that were missed. Plan on continuous improvement. A continuity plan is not a checklist item that is done once and then filed – it needs to be maintained, fine-tuned, periodically revisited, and adapted to your changing situation.

Your business continuity plan is one item that really should be kept on the cloud, or on a colocation server, with access set up so all the critical participants can access it. Don't make the mistake of assuming that the binder on the third shelf will survive the fire.

You will also hant to have remote copies on a cloud service for license information, software and hardware support contracts, client/vendor contact information, hardware inventory, plotter configurations, and your company standards documents. Scan the paper documentation, zip up the spreadsheet, pdf documents, and configuration data files, and park them safely.

Strategies for Design Data Recovery

The final element of your disaster recovery plan is the recovery phase. And the first step in that is damage assessment and salvage. Evaluate the assets that remain, determine if they are usable, or salvageable, and compare them to the inventory.

You should plan on not having any of your existing infrastructure available; assume that the servers, workstations, and on-site data has been completely destroyed. You need to work out a plan before hand for replacement, whether purchasing new equipment or leasing it on a temporary basis. Your servers, workstations, switches, may be fully functional, but don't plan on it ever working out that way, or staying that way. Whatever extreme event you are trying to recover from may have impacts that are not obvious, ones that will cause the hardware to fail hours, days, or weeks later.

If your off-site backups are current, and you've got hardware functioning that you can restore onto, then you're halfway there. If you followed the 3-2-1 rule, then you're probably in good shape as far as having readable and restorable data for active projects.

There is no magic bullet – the recovery phase is going to be problematic. Expected glitches and missing pieces. You will have to work around the issues that crop up as the present themselves– from unreliable power to unpredictable crashes. If you're running current versions of your design software, you'll be able to replace the software by downloading fresh versions. If you're running a network license server, and have to replace the server hardware, contact your reseller to get running quickly. If there are problems or delays, think about installing temporary trial versions of the design software on stand-alone workstations, and stock up on thumb drives for sneakernet.

And always, remember the "6 Ps"; Proper Prior Planning Prevents Poor Performance.

Checklist		
	Does the plan consider all natural or man-made emergencies that could disrupt your operations?	Pandemic, fire, explosion, flood, hurricane, earthquakes, toxic material releases, workplace violence, civil disturbance.
	Does the plan consider all potential internal sources of emergencies that could disrupt your workplace?	Conduct a hazard assessment of the workplace to identify any physical or chemical hazards that exist and could cause an emergency.
	Does the plan consider the impact of internal and external emergencies on the workplace's operations and is the response tailored to the workplace?	Brainstorm with the stakeholders asking what you should do and what would be the likely impact on your operation, and devise appropriate responses.
	Does the plan contain a listing of key personnel with primary and alternate contact information?	Keep the list current, and provide for an emergency communications system (cell phone, mobile radio)
	Does the plan list contact information for fire, police, and other first responders?	Keep the list current, ensure that emergency services can be contacted.
	Does the plan include the names, titles, departments, and telephones numbers of individuals to contact for additional information or decision making authority?	List the names and contact information for the responsible persons.

	Does the plan address rescue operations or medical assistance?	Most small employers will rely on public resources for these services, but first-aid training is available from the American Red Cross, or other local organizations.
	Does the plan identify how or where personal information on employees can be obtained in an emergency?	HR information is confidential, however in an emergency it can be vital to access important personal information, home & mobile phone numbers, emergency contact numbers,, next of kin, and medical information.
	Does the plan identify conditions under which evacuation would be necessary?	The plan should identify the scearios where workplace evacuation is required. This could include fire, chemical spill, flooding or earthquake. The extent of evacuation may be different for different types of hazards.
	Does the plan identify a clear chain of command and designate a person and alternate to order an evacuation or shutdown?	The person designated should have the authority and familiarity with the organization to lead and coordinate an evacuation or shutdown of the operation. An alternate should be identified for those instances when the primary leader is unavailable.
	Does the plan address the types of actions expected of different employees for the various types of potential emergencies/	A fire or earthquake would normally call for evacuation to the outside. A tornado or sudden severe storm may call for evacuation to a sheltered are within the building.
	Does the plan identify who, if anyone, will remain behind to shutdown critical equipment and operations during an evacuation?	All individual delaying their evacuation to shut down equipment or utilities such as gas or electric must be capable of knowing when to abandon that operation or task and evacuate themselves.

	Does the plan identify evacuation routes, and are those routes prominently posted in the workplace?	Create floor diagrams that designate exit routes from all locations, and include assembly points for staff to gather upon evacuating. Emergency egress routes should be well lit, clearly marked, wide enough to accommodate all personnel, clear of debris and obstruction at all times, and unlikely to expose personnel to additional hazards.
	Does the plan address procedures for assisting people during evacuation, especially those with disabilities or language barriers?	Designate reliable staff members to act as evacuation wardens to help move people from danger. One warden for every twenty people should be adequate, and the required number of wardens should be available at all times during working hours. Wardens should be tasked with checking office, cubical, break rooms, and restrooms in the event of an evacuation order.
	Does the plan identify one or more assembly areas where employees will gather, and is a procedure in place to account for all employees?	Accounting for all affected individuals is critical. Confusion in the assembly are can lead to delays in rescuing anyone trapped in the building, or to unnecessary search-and-rescue operation. Take a head count after evacuation and identify everyone in the assembly area. The names and last known location of any missing persons should be reported to the official in charge.
	Does the plan include provisions for tracking visitors?	Some organizations have all visitors sign in when at the facility. The hosts for the visitors, or evacuation wardens should be tasked with evacuating these individuals safely.
	Does the plan identify a preferred method for reporting fires or other emergencies?	911 is often the preferred method of reaching external first responders, and internal numbers may be used. Internal numbers can be connected to paging systems to alert personnel to an emergency.

	Does the plan describe the method to alert employees, including disabled worker, to evacuation or take other action?	Make sure that alarms are distinctive and recognized by all employees as a signal to evacuate the area or take other action prescribed in the plan. Ideally alerts should be heard, seen, or otherwise perceived by everyone in the workplace, including those who may be blind or deaf. Evacuation wardens can be tasked with ensuring that disables personnel are properly taken care of.
	Does the plan identify how and when employees will be trained so that they understand the types of emergencies that may occur, their responsibilities, and actions outlines in the plan?	Training should be offered to employees when you develop the initial plan, and as new individuals are hired. Retraining should occur when the plan changes due to facility changes, new equipment, hazardous material, or processes that affects evacuation routes, or when new types of hazards are introduced that require special handling.

	Does the plan indicate the types of training employees will be offered?	General training should address the following: • Individual roles and responsibilities • Threats, hazards, and protective actions • Notifications, warning, and communications procedures • Emergency response procedures • Evacuation, shelter, and accountability procedures • Location and use of common emergency equipment • Emergency shutdown procedures Additional train could include first aid, CPR, portable fire extinguisher use
	Does the plan describe when and how often retraining will be conducted?	Consider retraining on an annual basis, without reinforcement training will be forgotten
	Does the plan address if, when, or how often drills will be conducted?	Once the plan is in place, and workers are trained in their responsibilities, it is a good idea to hold practice drills as often as necessary to keep employees prepared. If possible, enlist outside resources such as fire or police. After a drill is completed, gather management and staff for an after-action assessment of the drill. Identify strengths and weaknesses of the plan, and improve it.