Architecture: Best Practices for Archiving Digital Design

Risk analysis,resources & best practices for archiving digital files safely & correctly.

White Paper

CRA
Transform IT
Computer Resources of America

Introduction

The days of storing huge paper archives are soon to be a thing of the past. In many ways this is an amazing advancement and testament to technology. The work that goes into archiving paper is unwieldy and high risk: from natural disasters to materials used. There are numerous legal issues with it that it adds extensive costs to architectural and design firms. Digital archiving is far more cost and materials effective - there's no need for special storage facilities which require special lighting, hiring staff, and temperature and humidity control - but there are still risks involved. It's important to hold digital archiving to high standards to avoid serious issues.

In this white paper we summarize:

- **Digital Archive Risks** - Learn the risks of digital archiving so that your firm is better equipped to put safeguards into place.

- **Best Practices for Archiving Digital Design Files** - Don't reinvent the wheel; there are accepted practices that will make digital archiving a better and more secure process.

- **Resources for Digital Archiving** - Finally, we'll share excellent resources to help with improving your current system or moving to one if you're still dealing with paper (even if you have a hybrid system now).

Digital Archive Risks

The risks to digital archives fall into two large categories: physical and digital. Even though a digital archive is just that, there are still physical risks that must be considered when creating policy and procedure. It can be easy to forget that.

Physical Risks

External hard drives can be lost, stolen or damaged. Many large firms allow architects and other staff to use external hard drives to store files, including for archiving purposes. These small drives make it easy to transport and backup large files. The fact that they are on a physical drive, though, opens them for the risk of them being lost, stolen, or sustaining damages.

External drives should be governed by strictly enforced policy and procedure. Computer Resources of America recommends requiring that drives be locked in safes whenever the professional is away from their desk. When traveling these items should be required to not be in laptop bags but in checked or carry on baggage. This is because travel-related thefts see laptop bags getting swiped more than anything else. These bags are generally light and easy to grab.

Back everything up twice. Even cloud storage has a physical genesis. When this is on a server farm or on site, these locations are subject to natural disasters like floods and extreme weather. Multiple backups means less risk for loss due to acts of God.

Train all staff and offer refreshers. Make training staff on your archive procedures a mandatory part of new employee orientation. Anyone with access to the archive or who accesses files themselves must be trained in how to do this safely and in line with your archiving protocols to make sure that human error doesn't result in data loss. CRA suggests refreshers for staff. It can be as simple as a 15 minutes lunch and learn session or part of annual review meetings. In addition to making sure everyone has the required knowledge of procedure this also shows you take your archives seriously and expect everyone else to.

Digital Risks

The biggest digital risk to archives are cyber attacks like malware, ransomware and other hacks and viruses.

Don't let archives go dark. A risk many aren't aware of is that that comes with untouched archives. As completed projects fade into memory, their archives aren't accessed. These dark archives are ripe for cyber attacks. Once hackers know that these areas are not accessed they become prime targets for finding information.

Apply the same cybersecurity protocols to archives as you do live files. Don't forget to apply the same protocols you do to your network and cloud as you do to your archives. This is imperative to staying safe. It can be easy to forget archives since they are no longer files you're using regularly but they are just as important as when they are active files as when they've been stored.

Digital Archive Best Practices

Here's a quick, at-a-glance version of recommended best practices all architectural firms should consider implementing.

For Physical Drives

Have two back ups. Remember, risks exist! Always have one cloud and one physical drive backup of everything. If it's stored anywhere, three copies should exist. One in its native location, one in your cloud, and one on a secured external drive.

Store Properly. Have safes on site for storing external drives that are not attended to. It's easy to pop them in at the end of the day and a safe with shelves helps keep it organized. This safe should be locked. Look around the next time you're at a bank or other office with safes. Many are left open for ease. But the reason we have safes is to keep things safe. And that can only help when they are secured all the time.

It may seem to make sense to keep a safe open during the day to save time. It's not. The IBM X-Force® Research 2016 Cyber Security Intelligence Index reports 60% of attacks originate from ***inside the attacked organization.***

Require professionals who travel and/or commute with external drives to never keep these in their laptop bags and use a locked safe at home and in hotels.

Policy/Procedure

Take time to develop - preferably with the guidance of experts - policy and procedure that is smart, efficient and shows the importance of archive security to all in your organization. Include all the recommendations above.

It's not just about safety, though, there is something else to consider with archiving.

First, make sure that files are saved in a uniform way with a specific naming/file/folder structure. This guarantees that in the event of anything from drawing from a project that has received accolades in a proposal, presentation or pitch it can be found quickly and easily. Alternatively, in the unfortunate event of a problem or lawsuit you can also have necessary documentation on hand. Nothing is more damaging to a firm that clients and prospective clients viewing them as disorganized.

Cloud Archives

Safety/Security - Are you regularly monitoring access to your cloud? Are you checking for interlopers? Monitor your cloud storage regularly. Have an outside firm or in house staff monitor archives the same way they do the in house network that is used daily.

Consider Software - Unless you're tiny, Google Drive isn't going to cut it for archiving. Consider software to help. AutoDesk is a favorite among architectural firms. You can also work with an outside contractor to build you a custom archive system including naming conventions and helpful "ReadMe" files that will help enforce uniformity and organization.

There are outside firms that will also handle your archive storage needs on their servers.

Policy/Procedure - There are many ways to write policy but here are our five tips for starting to build a sound policy for protecting your archives.

1. **Password Protect.** All archives should be password protected using a separate password for individual users different than their regular login.
2. **Regulate Passwords.** Don’t just require a password. People are awful at picking passwords. Require long passwords that include no consecutive letters that form words including using numbers and symbols to replace letters. Require caps, lowercase and special characters. Finally, make sure that passwords are changed regularly - every 3 to 6 months.
3. **Control Access.** In today’s more collaborative culture it feels strange at times to be super strict with employees, almost like micromanaging. It is perfectly fine to be strict when it comes to security. Make sure that employees know to only access archives from safe connections and devices and never over unapproved devices or public access.
4. **Put those storage regulations in writing.** Don’t just talk to employees about safes and traveling with drives in a carry on bag - put this into the policy so that it takes on importance.
5. **Stay up to date.** Threats and tactics change. Make sure your organization works with trusted industry experts to stay on top of the best practices.

Resources for Digital Archiving Help

Computer Resources of America provides cloud storage and outsourced dedicated IT services to companies in the greater New York City metropolitan area, New Jersey and Connecticut. Contact us to learn how we can assist you in setting up, maintaining and regulating your digital archives and how our team of professionals can provide the necessary IT services and solutions for your business.

CRA™
Transform IT
Computer Resources of America

Corporate Headquarters

64 West 48th Street, New York, NY 10036 – 212-376-4040 – www.consultcra.com – sales@consultcra.com