LeadingIT

July 2025

The NetWork

- BLUEPRINTS TO BACKUPS: HOW AEC FIRMS CAN PROTECT THEIR PROJECT DATA
- WHY ONE-CLICK EMAIL ATTACKS ARE YOUR BIGGEST LIABILITY
- THE SMARTEST WAY TO ORGANIZE SHARED FOLDERS (AND STOP LOSING FILES)
- IT SUPPORT FOR NONPROFITS: HOW TO SECURE DONOR DATA WITHOUT BREAKING THE BANK

Blueprints to Backups: How AEC Firms Can Protect Their Project Data

In architecture, engineering, and construction (AEC), data is the foundation of every project. From CAD files and BIM models to project timelines and financial documents, the information you generate and manage is critical not just to project success, but to your firm's reputation, operations, and bottom line. With cyber threats on the rise and project data becoming a prime target, AEC firms must prioritize data protection like never before.

The Value and Vulnerability of AEC Data

AEC firms rely on vast amounts of sensitive data. Floor plans, blueprints, client contracts, 3D models, and proprietary designs are not only intellectual property, they are often essential to daily operations and client trust. A single ransomware attack or accidental data loss could stall a project, breach contracts, or cost millions in recovery and lost business.

According to Egnyte's 2024 AEC Data Insights Report, 77% of firms say they cannot endure more than five days without access to documents during a ransomware attack. Yet, such attacks can lock teams out for 20 days or more. That kind of disruption can bring entire projects to a standstill.

The threat is more than theoretical. In the past two years, 59% of AEC firms experienced a cybersecurity incident, with general contractors facing the greatest impact. Seventy percent reported a cyber event, and 30% were hit by a ransomware attack since 2021. These numbers reflect the growing vulnerability of the industry as it increasingly adopts digital workflows.

Common Threats to Project Data

AEC firms face a mix of internal and external risks:

- Ransomware attacks targeting project files and backups
- Phishing emails tricking staff into exposing login credentials
- Insider threats from untrained employees or disgruntled former staff
- Hardware failure or natural disasters leading to data loss
- Unsecured mobile devices or Wi-Fi networks used on job sites

Compounding these threats is the highly collaborative nature of AEC projects. Architects, contractors, engineers, and clients regularly access and modify project files from multiple locations and devices. When firms rely on outdated IT systems or unsecured file-sharing tools, they increase the risk of unauthorized access, accidental deletions, and data exposure.

The complexity and mobility of AEC work make it essential to implement layered protections that account for these varied vulnerabilities.

Protecting Data from the Ground Up

Data security doesn't have to be overwhelming or expensive, it just needs to be strategic. Here's how AEC firms can start building a strong data protection foundation:

1. Use Cloud-Based Collaboration Tools Wisely

Platforms like Autodesk Construction Cloud, Procore, or Microsoft 365 provide secure collaboration environments with access controls and version tracking. Ensure these tools are properly configured, and limit access based on user roles and project needs.

2. Implement Strong Access Controls

Not every team member or partner needs access to all project files. Use role-based permissions to control who can view, edit, or share data. This reduces the risk of accidental changes or leaks.

3. Train Teams on Cyber Hygiene

Human error is a leading cause of breaches. Conduct regular training on spotting phishing attempts, using strong passwords, and safely accessing project files from mobile devices or remote locations.

4. Regularly Back Up Your Data

Don't just rely on local servers or individual devices. Implement automatic, encrypted backups both onsite and in the cloud. Test recovery procedures regularly to ensure backups are accessible when needed.

5. Use Multi-Factor Authentication (MFA)

MFA can prevent 99.9% of account compromise attacks, according to Microsoft. It's a low-cost, high-impact safeguard that every AEC firm should implement.

Conclusion: Build Security Into Every Project

As AEC firms continue to embrace digital workflows, safeguarding that data must be baked into every phase of the project lifecycle. From blueprints to backups, every file matters. And with the right safeguards in place, you can build with confidence knowing your data is as secure as your design.

IT Support for Nonprofits: How to Secure Donor Data Without Breaking the Bank

Nonprofits face a unique challenge. You're mission-driven, resource-conscious, and focused on impact. But with limited budgets and lean teams, investing in high-end cybersecurity tools often feels out of reach. Yet, one area that can't afford compromise is data security, especially when it comes to sensitive donor information. The good news is you don't need a massive budget to stay protected. With strategic choices, even small to mid-sized nonprofits can secure donor data effectively.

Why Donor Data Security Matters

Donors are the lifeblood of your organization. They trust you not only with their money but also with their personal information, including names, addresses, and payment details. A breach doesn't just result in financial loss; it erodes trust and damages your reputation. Cybercriminals are increasingly targeting nonprofits, knowing that many lack strong cybersecurity defenses.

Here are a few things to consider:

1. Start with Simple, Low-Cost Security Basics

Some of the most effective cybersecurity practices are also the most affordable. Here are a few key practices that should be in place:

- Use strong passwords and require staff to update them regularly. Consider a password manager to encourage the use of strong passwords. Many offer free or nonprofit-friendly plans.
- Enable multi-factor authentication (MFA) wherever possible; especially on email, cloud storage, and donor databases.
- Keep software up to date, including operating systems, browsers, and antivirus tools. Automatic updates are often available and easy to turn on.

2. Take Advantage of Free and Discounted Tech

Many major tech companies offer free or deeply discounted services to nonprofit organizations. Through platforms like TechSoup, nonprofits can access:

- Microsoft 365 for Nonprofits, which includes secure email and cloud tools
- Google Workspace for Nonprofits, with document sharing and security controls

These tools often come with built-in security features that are sufficient for many nonprofit needs, especially when properly configured.

3. Limit Access to Donor Data

Every staff member or volunteer doesn't need access to all donor records. Setting up role-based access controls can reduce the risk of accidental data exposure or internal misuse. Many donor management systems (like Bloomerang, DonorPerfect, or Little Green Light) include permissions settings that are easy to configure.

4. Train Your Team to Spot Red Flags

Human error remains the leading cause of data breaches. Equip your staff and volunteers with the skills to recognize and respond to threats, like:

- Identifying phishing emails
- Using secure file-sharing practices
- Safely handling personal data

Free training resources are available through organizations like the National Cybersecurity Alliance.

5. Back Up Your Data Regularly

Data loss can happen from a cyberattack, hardware failure, or even human error. Set up automatic, encrypted backups to both local and cloud storage. Free or low-cost tools like Google Drive and OneDrive can do the job without much technical setup.

6. Consider Scalable Support When You Need It

As your nonprofit grows or faces more complex challenges, consider partnering with a managed IT services provider that can offer:

- Ongoing monitoring
- Strategic guidance
- Help desk support
- Proactive cybersecurity planning

It's a flexible, scalable solution that allows you to access expertise without hiring full-time IT staff.

Conclusion: Protecting Donor Trust Starts with Practical Security

Securing donor data doesn't require a major investment, just the right mindset, and a few smart practices. By starting with free and low-cost tools, training your team, taking advantage of nonprofit discounts, using smart strategies, and getting expert support when you need it, your organization can protect its data, preserve donor trust, and focus on what matters most: your mission.

The Smartest Way to Organize Shared Folders (and Stop Losing Files)

Let's be honest — shared folders often feel like digital junk drawers.

You open a drive to find 42 versions of the same file, a sea of unlabeled PDFs, and a folder named "Old Stuff – Do Not Delete (Maybe?).pdf" that's still mysteriously critical to operations. If this sounds familiar, you're not alone! Disorganized shared folders slow teams down, lead to costly mistakes, and turn simple file-finding into a scavenger hunt. But the fix? It's easier than you think and doesn't require any special software.

Here's how to organize your shared folders in a way that makes sense, saves time, and keeps your team on the same page.

1. Start with a Simple, Standardized Folder Structure

Create a top-level folder system that mirrors how your business operates.
Ex:

- 🗂️ Finance
- 🗂️ HR
- 🗂️ Marketing

Under each, add clear subfolders by year, project, or client name, whatever's easiest for your team to follow.
Pro tip: Don't over-nest. If it takes more than 3 clicks to get to a file, it's buried.

2. Name Files Intentionally (So People Can Find Them Later)

Stop with the "Final_v2_REALLYFINAL.docx" chaos. Use a consistent naming format like:

[Project/Client] – [File Name] – [Date or Version]
Ex: 📄AcmeInc–WebsiteProposal–2024-05-01.pdf

This makes files easy to scan and search even without opening them.

3. Set Permissions Based on Roles, Not Individuals

Too often, everyone has access to everything. That's a risk and a recipe for accidental deletions.
Set access based on roles (e.g., "Marketing Team" or "Managers") using group permissions in Microsoft 365, SharePoint, or Google Workspace. That way, when people join or leave, access is handled cleanly.

4. Schedule a Monthly or Quarterly "Drive Clean-Up"

Assign someone (or rotate the responsibility) to archive old files, merge duplicates, and delete outdated content.
Use an "Archive" folder with read-only access for anything that shouldn't be deleted but doesn't need daily use.

5. Document Your Folder Rules & Share with the Team

Even the best system fails if no one follows it. Create a short, friendly file management guide. Keep it light and simple. Think:

- Where to save new files
- What naming format to use
- Who to ask before creating a new folder

Bonus: Add it as a pinned message in Teams or Slack.

Why One-Click Email Attacks Are Your Biggest Liability

It only takes a single click to trigger a devastating cybersecurity incident. One-click email attacks, where a user clicks a malicious link or opens a harmful attachment, remain one of the most common and damaging cybersecurity threats. These attacks are simple, effective, and alarmingly easy to fall for, especially when employees are unprepared to spot them.

What Is a One-Click Attack?

One-click attacks often start with phishing emails. These emails are designed to trick users into clicking a link or downloading a file that installs malware or leads to credential theft. The emails can look like messages from trusted sources, including banks, colleagues, or well-known companies.

Once the user clicks, the damage is done. Cybercriminals may gain access to sensitive information, install ransomware, or hijack internal systems without the user realizing what happened until it is too late.

Why Are One-Click Attacks Effective?

One-click attacks work because they target people, not just systems. Even tech-savvy users can be fooled when they are rushed, distracted, or under pressure. Phishing messages often use urgent language, fake alerts, or emotional appeals to prompt quick action.

The problem is only getting worse. In 2024, phishing click rates tripled compared to the previous year. This sharp rise shows that traditional awareness training isn't enough. Even tech-savvy users are falling for more advanced and convincing phishing schemes.

Many businesses also lack key protections such as email filtering, multi-factor authentication, or user training. Without these defenses in place, a single click from one employee can result in a major breach.

The Real Cost of One Mistake

A single click can lead to severe consequences. According to the 2024 IBM Cost of a Data Breach Report, the average global cost of a breach is $4.9 million. Even for smaller organizations, the financial and reputational damage can be devastating.

Ransomware is a frequent outcome of one-click attacks. It can lock down systems, disrupt operations, and demand expensive payouts. In some cases, companies also face legal consequences or fines if sensitive data is exposed.

How to Reduce the Risk

You do not need a massive IT budget to protect your team. A few practical steps can go a long way in defending against one-click attacks:

- Train your staff. Regular security awareness training helps employees recognize phishing attempts and know how to respond.
- Use email filters. Advanced filtering tools can block many phishing emails before they reach inboxes.
- Implement multi-factor authentication. Even if login credentials are stolen, MFA can prevent unauthorized access.
- Keep software up to date. Ensure all devices have current security patches, antivirus software, and firewalls in place.
- Run phishing simulations. Periodic testing helps reinforce safe behaviors and identify training gaps.

Conclusion: Staff Training is Key

One-click email attacks are low-effort for cybercriminals but high-impact for businesses. They exploit your biggest vulnerability—human error—using tools that are readily available and constantly evolving. But by building a culture of security awareness, using smart tools, and staying proactive, your organization can significantly lower the risk. Cybersecurity is not just about technology. It starts with people, and the right training can be your strongest defense.

$1000 REFERRAL PROGRAM

Do you know an organization that needs unlimited IT and cybersecurity support with an unbeatable guarantee?

You'll earn **$50** for every referral. If they sign up, you'll receive **$1000!**

SCAN TO LEARN MORE

815-788-6041 GOLEADINGIT.COM/REFER

DRIVEN – CHASES EXCELLENCE – HUMBLY CONFIDENT – ACCOUNTABLE – STAYS POSITIVE

LeadingIT Core Values Victor of the Month

Laura Piekos, President

Congratulations to this month's Values Victor for being Accountable!

Please help us congratulate our latest Values Victor, Laura Piekos, for exemplifying what it means to be ACCOUNTABLE. Since joining LeadingIT in 2018, Laura has consistently led by example, owning outcomes, standing by our numbers, and doing whatever it takes to make IT right for our clients and team. As President, she sets the bar high and reminds us all that true accountability means taking ownership, learning from missteps, and never passing the buck. Way to go, Laura!

LeadingIT

We Help Chicagoland Organizations Eliminate Concerns Over IT and Cybersecurity Where the Unsolvable is Solved with Unlimited Support, and an Unbeatable Guarantee.

WE ARE CELEBRATING!

BIRTHDAYS

HISSAN BADAR	7/4
CHRIS HANSEN	7/9
SETH LAVIGNE	7/15

ANNIVERSARIES

LORI YARNALL	2 YEARS
DANIEL RABENOLD	2 YEARS
MATTHEW MCMULLAN	2 YEARS