Nonprofits

Tech mistakes Chicagoland **nonprofits can't afford to ignore**

Leading a nonprofit today means balancing mission work with budgets, grants, reporting, staff, volunteers, and the occasional "we need this now" request. You are also answering to donors, partners, and regulators who want proof you are running a tight ship.

In Chicago, where many nonprofits run lean teams and fast-moving programs, small tech issues can become mission delays quickly

Your technology should remove friction, not add it.

But when laptops crawl, files disappear, or email goes sideways, the whole organization feels it.

Most leaders did not sign up to babysit software. Still, the systems behind fundraising, case management, and finance are part of delivering services.

Cyber threats keep rising, stakeholders expect reliability, and your board (of directors) will assume you have covered the basics to protect data and keep operations moving.

Good IT is not about ripping and replacing everything. It is about getting the fundamentals right: secure access, predictable support, and backups that can actually bring you back after an incident.

The real role technology plays in nonprofit impact

Nonprofit work in has changed.

It rarely happens in one place, on a couple of office desktops.

Across Chicagoland, teams are spread across offices, homes, partner sites, and community locations, so your systems have to travel with them.

Your team is in the field, at partner sites, at events, on home Wi-Fi, and sometimes answering a donor or client question from a phone between meetings. Grant files, donor records, program notes, and financial reports get opened on laptops, tablets, and mobile devices at all hours.

That flexibility is a big win. It also breaks down fast when your systems were designed for a simpler, office-only world.

Older setups assume everyone is on the same network, using the same tools, with the same access patterns. Stretch that model across remote work and you get slow logins, awkward workarounds, and "temporary" shortcuts that quietly turn into daily habits.

Someone forwards a spreadsheet to a personal email "just to print it." A volunteer uses a free file-sharing app because it is easier. Program staff save documents locally because the shared drive is unreliable. None of it is malicious. It is the natural result of friction.

Meanwhile, cyber risk is no longer an occasional headline. It is part of normal operations.

Attackers go after nonprofits because you hold sensitive information, move money, and depend on trust and timelines. A phishing email that hijacks an inbox, a ransomware incident that locks up shared files, or a compromised payment process can stall services overnight.

And unlike many problems, a security incident is not easy to keep quiet. Donors, partners, clients, and your board (of directors) expect you to protect information and keep the organization running.

So, the question isn't ***"Does technology matter?"***

It's ***"Is your technology is dependable enough to support the mission, or if it is quietly working against you?"***

A clear map of your nonprofit IT

You do not need to be a technologist to run a strong nonprofit. But it helps to have a plain-English view of what is actually powering your day to day work.

Most nonprofits rely on the same core building blocks, even if the tools and vendors differ.

Where your files and key applications live

Every organization has a "home base" for documents and core systems. For some nonprofits, that is still a physical server tucked into a closet or a small server room. It may hold shared folders, line-of-business apps, or older databases that keep the lights on.

That approach can be perfectly workable when it is maintained well. The catch is ownership. Someone has to patch it, monitor it, back it up, and plan for replacement before it fails at the worst time.

Other nonprofits use hosted or cloud platforms instead. The outcome is similar, shared access to files and apps, just delivered from professionally managed infrastructure. You connect through the internet, and the underlying hardware maintenance is handled for you.

Neither option is automatically "better." What matters is knowing which model you are using, what it supports, what it does not, and who is accountable for keeping it healthy.

Donor, client, and program systems

In a nonprofit, the "system you live in" is often a donor database, CRM, case management platform, grant tracking tool, or a mix of all three.

On the surface, it is where people enter notes, log interactions, pull reports, and track outcomes. Behind the scenes, it is doing the heavy lifting that keeps programs consistent and fundraising organized. When it is configured well, it prevents staff from guessing which spreadsheet is current or where the latest intake form was saved.

The common issue is not that the software is bad. It is that organizations only use a small slice of what they pay for. Teams fall back to side spreadsheets, duplicate data entry, and manual steps that add time and create reporting headaches later.

Email and collaboration

For most nonprofits, email is still where decisions, approvals, and “can you send that right now” requests happen.

Modern platforms can do much more than move messages around. They can help you organize shared communication, reduce mistakes, support secure file sharing, and connect conversations to client records or donor histories when set up properly.

When those connections are missing, staff spend their time copying, pasting, re-filing, and hunting for context.

Wi-Fi and networking

Weak networks show up as slow systems, choppy calls, and the quiet frustration that makes people invent workarounds.

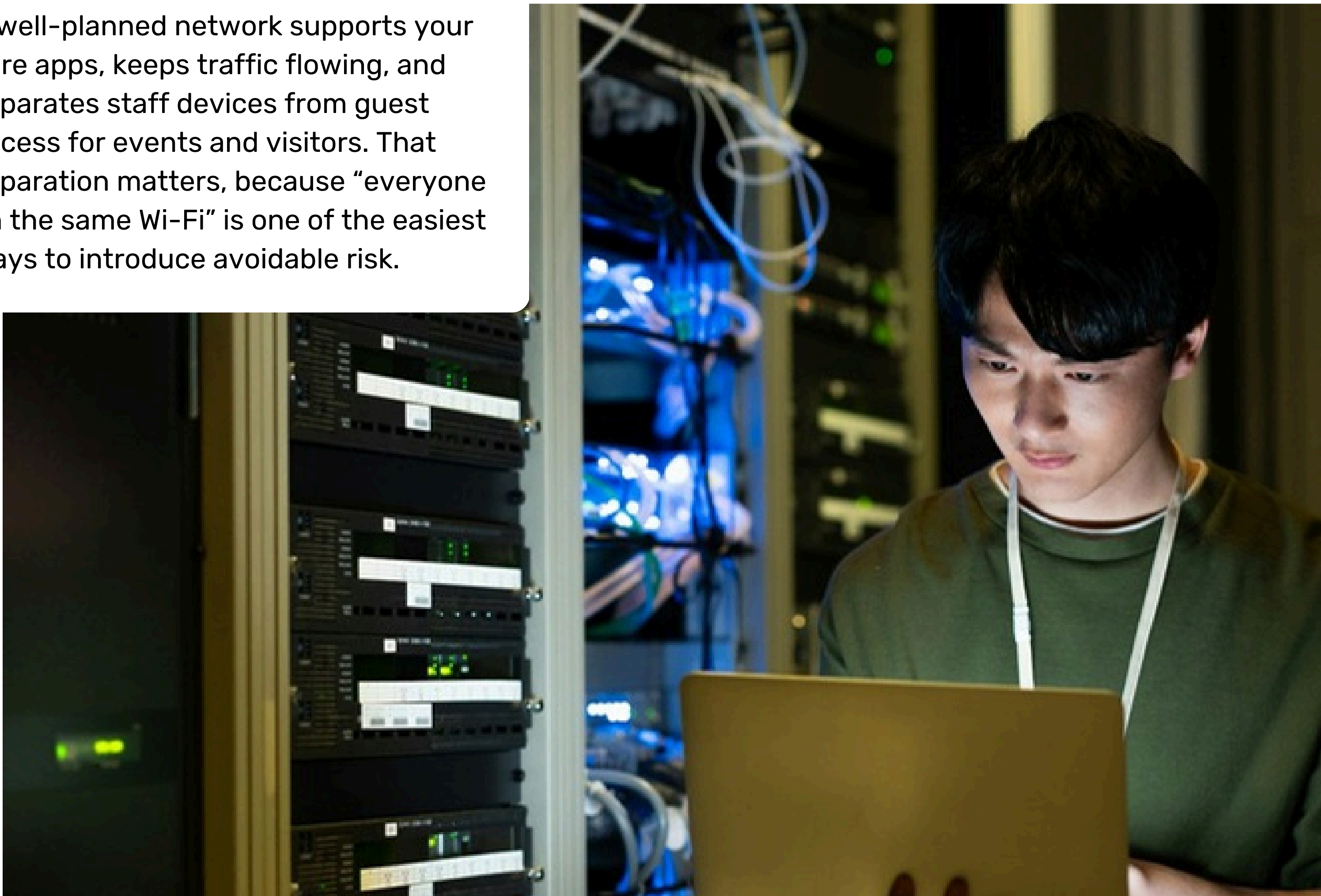
A well-planned network supports your core apps, keeps traffic flowing, and separates staff devices from guest access for events and visitors. That separation matters, because “everyone on the same Wi-Fi” is one of the easiest ways to introduce avoidable risk.

The cloud

The cloud is simply a way to store data and run systems in secure, professionally managed environments that you access over the internet.

Used thoughtfully, it often improves flexibility and resilience. It does not mean you lose control of your information. It means you choose the right controls, the right access, and the right protections, and you make sure someone is responsible for validating those choices.

Once you understand these pieces at a high level, you can ask better questions, spot weak assumptions, and make decisions your board (of directors) can feel confident in.



Security basics worth doing every time

Cybersecurity can sound like a specialty topic. For most nonprofits, real protection comes from doing a few unglamorous things consistently, not buying the flashiest tool on the market.

Start with access. Who can see what, and how do you know it is really them?

That is where strong sign-in practices matter. Use long passwords and back them up with multi-factor authentication (MFA). MFA adds a second proof, usually a prompt or code on a phone, so a stolen password is not enough to break in. It can feel like an extra step for staff, but it blocks a huge share of common attacks.

Next is encryption. Encryption scrambles information so it cannot be read if someone gets hold of a device or intercepts data in transit.

Modern platforms can encrypt laptops, phones, and stored files. If a device is lost or stolen, donor records, client notes, and finance documents are far less likely to become a public problem.

Encryption is often available by default, but it is not always turned on everywhere, or configured the same way across all devices.

Network safeguards are another quiet win. Firewalls and web filtering do a lot of work in the background.

A firewall sits between your systems and the internet and blocks suspicious traffic. Web filtering reduces the chances that staff land on known malicious sites or fake login pages, even when someone clicks the wrong link. Training still matters, but these tools give you a safety net when people are busy.

Device security matters just as much as what happens in the cloud or on a server.

Work happens across laptops, phones, and tablets, including personal devices.

Those endpoints should be updated, protected with passcodes or biometrics, encrypted, and monitored by whoever supports your IT. Allowing personal devices “for convenience” without clear rules is one of the fastest ways for sensitive data to drift into places you cannot control.

Then there is phishing, the everyday tactic criminals use to trick real people through email and messaging.

The bait changes constantly: a shared document link, a vendor invoice, a password reset notice, a note that looks like it came from your Executive Director, or an urgent request tied to payments. The goal is always the same: get someone to click, enter credentials, or open something dangerous. Teaching staff to slow down, verify, and report anything that feels even slightly off is one of the most cost-effective defenses you can put in place.

None of these steps are exciting. Together, they reduce risk in practical ways and give your board (of directors) confidence that the organization is taking reasonable precautions with the information and resources it is trusted to protect.

> ***“Chicago nonprofits are not ‘too small to matter’ to attackers, especially when email and shared files touch donor funds and client data.”***

Making data protection part of how you work

Data protection is rarely one big decision. It is the small, repeated choices: where information lives, who can open it, and how long you keep it.

A simple place to start is access control.

Not everyone needs access to everything. When you intentionally limit access by role, you reduce the blast radius of everyday mistakes and more serious problems like a compromised login or an unhappy former employee.

Retention is another area where nonprofits drift into trouble without meaning to.

Old client notes, volunteer applications, donor exports, and “final” grant drafts tend to stick around forever. Over time, that creates a growing pile of sensitive data that can be exposed if something goes wrong. Clear retention rules, plus a routine for archiving or deleting, keeps your footprint reasonable and your reporting cleaner.

Storage choices matter just as much as retention.

Mission-critical documents should live in approved, secured systems, not scattered across personal inboxes, USB drives, or random cloud folders created for convenience.

The moment information moves outside what your IT support partner can monitor and protect, you lose visibility, consistency, and control.

It also helps to define how data is shared.

If your team regularly sends spreadsheets with personal information, copies client documents into email threads, or forwards attachments to vendors, write down the approved method and make it easy to follow. The goal is not to police people. It is to remove ambiguity so the safest option is also the simplest option.

When something does go wrong, planning beats improvising.

An incident response plan does not need to read like a legal contract. It can be a one-page playbook that spells out who owns the response, what happens first, who gets notified, and how decisions are documented. That clarity reduces delays when minutes matter.

Documentation ties everything together.

When expectations are written down and kept current, people can act consistently even when they are busy, new, or working remotely. Onboarding goes faster, and if your board (of directors) ever asks how you protect donor, client, and operational data, you have something specific and credible to point to.

Keeping email and file sharing from becoming a risk

In most nonprofits, the real work moves through inboxes and shared files. That is also where many security and privacy issues begin. Not because email or document tools are "unsafe," but because they get used for everything.

A common trap is letting email become the default solution. It turns into the place you send draft grant narratives, share donor lists, request approvals, pass along participant updates, and forward documents to partners. The more jobs email is asked to do, the easier it is for something to slip. A file goes to the wrong person, an internal comment is included by accident, or a long thread contains details the recipient never needed to see.

Whether you're coordinating services across Chicago or collaborating with partners statewide, sharing links from approved systems beats forwarding attachments

A safer approach is to keep sensitive information in systems built for controlled access, then share links, not attachments.

That can look like a secure folder with permissions, a shared workspace where files have one "home," or a portal inside your donor CRM, case management, or grant platform. When information stays in one managed place, you can set who can view or edit it, remove access when roles change, and avoid endless copies bouncing around email.

Version control matters just as much as security.

If the same document exists in five inboxes, two desktop folders, and a shared drive, someone will eventually send the wrong one.

Systems that maintain a single source of truth, show who changed what, and allow easy rollback quietly prevent confusion. They also reduce the late-night scramble to figure out which file is final.

Messaging apps can create similar problems.

Texting and consumer chat tools feel fast and familiar, especially with volunteers, donors, and community partners. But they are rarely designed for organizational record-keeping, consistent access control, or offboarding when someone leaves. Conversations may live on personal phones, sync to personal cloud backups, and disappear when you need them most. It is usually better to guide people toward approved tools your organization can manage and retain appropriately.

Finally, remember that many leaks are simple human mistakes. Autocomplete picks the wrong "Mike," a link is shared too broadly, or an old email is forwarded without noticing what is below it. Clear standards, built-in warnings, and a culture that encourages a quick pause and double-check can prevent a lot of avoidable damage.

On-site, cloud, or hybrid: what fits your nonprofit

A common question for nonprofit leaders is where your core systems should run: on equipment in your office, in the cloud, or split between the two.

Keeping a server on-site can feel straightforward. You can point to it, you “own” it, and it may seem like the simplest way to run shared files or an older line-of-business application. That sense of control comes with real responsibility, though. You need a plan and budget for hardware replacement, power, cooling, security, monitoring, backups, and regular updates. When on-site systems are cared for properly, they can be fast and dependable. When they are not, issues tend to surface suddenly, usually when your team is busiest.

Cloud services shift most of that upfront cost into a subscription model. Instead of buying and maintaining hardware, you pay monthly for professionally managed infrastructure. Capacity is often easier to adjust as programs expand, staffing changes, or a new grant adds reporting requirements. For organizations that operate across locations, support hybrid work, or rely on volunteers and partners, cloud access can also be simpler to manage since people can securely reach the same tools wherever they are. Likewise, for organizations serving clients across the Chicago metro, cloud access can simplify secure collaboration without depending on a single office network

Security is not automatically better in one approach than the other. Both can be safe or risky depending on how they are configured and maintained. Cloud providers typically invest heavily in physical security, redundancy, and monitoring that is difficult for a single organization to match on its own. On-site environments can be highly secure too, but only when someone is actively managing patching, access control, and ongoing maintenance.

Whatever model you choose, avoid one dangerous assumption: that the platform will “handle it” on its own. Backups, updates, and monitoring still need to be designed, tested, and owned, with visibility your board (of directors) can trust.

Backups and continuity when things go sideways

Nobody enjoys imagining a crisis. But for a nonprofit, planning ahead is almost always cheaper, calmer, and far less disruptive than trying to invent a response while services are stalled.

Backups are the starting point. A backup is an extra copy of your information that you can restore when something gets deleted, damaged, or locked up.

If there is only one copy of a file, whether it sits on a laptop, an office server, or inside a cloud platform, it is not truly protected. Devices fail. Accounts get compromised. Someone clicks the wrong thing. People leave and access gets missed. The causes vary, but the outcome feels the same when the data is suddenly out of reach.

A practical way to think about backups is the 3-2-1 approach. Keep **three** copies of important data, stored on **two** different types of storage, with **one** copy kept off-site.

In real terms, that might look like your primary system, a second copy on a dedicated backup device, and another copy stored securely in the cloud. The point is to avoid a single point of failure, especially when the unexpected shows up at the worst moment.

Ransomware makes this painfully clear.

Ransomware locks your files and demands payment to unlock them. If you have recent, clean backups that are isolated from everyday access, you can wipe affected systems and restore what you need. Organizations that feel forced to pay often discover their backups were incomplete, outdated, or connected to the same environment that got infected.

Backups only solve part of the problem, though.

They protect your data. They do not automatically protect your ability to keep operating while systems are down.

That is where business continuity comes in. Continuity planning answers questions like: “If our systems went offline today, how would we keep supporting clients and running programs?” and “How quickly do we need to recover before it impacts funding, safety, or trust?”

There is no universal right answer.

Some nonprofits can absorb a day of disruption. Others cannot. The key is to define your tolerance for downtime and data loss, then make sure your backup and continuity plans are designed to match, and reviewed with your board (of directors) so expectations are clear before the pressure hits.

Using automation and smart tools to reduce admin

So far, a lot of this has been about preventing problems. That matters. But technology should also make the organization run smoother and free up time for mission work.

Many nonprofit workflows are more repeatable than they look. New clients are onboarded in similar ways. Donation acknowledgments follow a pattern. Volunteer intake requires the same steps. Grant reporting pulls from the same sources. Board packets get built on a predictable cadence.

When those processes live in people's heads or scattered checklists, they take longer than they should and create room for missed steps. Something gets skipped, duplicated, or done late, not because anyone is careless, but because everyone is busy.

Workflow automation helps your systems handle the repeatable parts.

For example, a new client intake can automatically create the right folders, assign tasks, and notify the right staff.

A donation can trigger a thank-you email, a receipt, and a follow-up reminder without someone manually copying information between tools. A grant deadline can generate a timeline of tasks with owners, so progress is visible before the week it is due.

Your team still makes the decisions. Automation just removes the predictable admin that drags people away from programs and relationships.

Templates are another practical win that many organizations underuse.

Standardizing donor letters, program forms, common email responses, policies, and board materials reduces rework and keeps messaging consistent. It also lowers the chance someone grabs an old version from a desktop folder and sends it out with outdated numbers or language.

Newer tools, including AI assistants, can also help when used carefully. They can summarize long reports, turn meeting notes into action items, propose first drafts of routine communications, and help staff find relevant information faster. The key is guardrails. Use these tools inside secure, controlled environments with clear rules about what data they can access and what should never be pasted into a public tool.

Search is the other quiet time-saver.

Good search can index shared documents, emails, and knowledge bases so staff can find what they need quickly, instead of hunting through folders or reopening old threads.

That saves minutes that add up, especially for leadership and operations teams. Collaboration tools and e-signature platforms can remove delays tied to printing, scanning, and tracking approvals. That is useful for vendor paperwork, HR documents, program agreements, and board votes where speed and clarity matter.

Voice dictation is another simple advantage, especially for staff in the field. If people speak faster than they type, dictating notes and converting them to text can reduce end-of-day paperwork and help keep records timely.
None of these tools replace people. They reduce low-value work, tighten consistency, and give your board (of directors) more confidence that the organization can scale its impact without scaling chaos.

Keeping access tight as your team changes

As your nonprofit grows and people cycle in and out, it gets harder to answer two basic questions: who has access to what, and from which devices?

That is where Mobile Device Management (MDM) helps. An MDM platform gives your IT support partner a central view of the laptops, phones, and tablets that connect to your systems. It can enforce encryption, confirm security updates are applied, and remotely lock or wipe a device if it is lost or stolen.

This matters even more when staff and volunteers use personal devices. Without clear controls, work files and email can blend into personal apps and storage. When someone leaves, there may be no clean way to remove organizational data without relying on goodwill and memory.

Access control is the other half of the picture. The safest approach is to give people the minimum permissions they need to do their job well. That keeps sensitive donor, client, and financial information from spreading across the organization without a reason.

Over time, access tends to grow "just in case." If nobody reviews it, you can end up with staff accounts that see more than they should, shared logins that never get retired, and old accounts that were not properly closed when roles changed.

Offboarding needs to be disciplined.

When someone leaves, their accounts should be disabled quickly, company-owned devices collected or securely wiped, shared passwords changed, and access to key tools reviewed. Leaving accounts active "for now" because they might be useful later is one of the easiest ways to create hidden risk.

Regular account and permission reviews are a simple habit with a big payoff. If an account does not have a clear owner or purpose, it is usually better to remove it than let it quietly linger. Your board (of directors) will expect that level of basic hygiene.

How to evaluate your IT support partner

Even well-built systems will have issues from time to time. What matters is how they are handled, and whether small problems are caught before they turn into big interruptions.

That is why your IT support partner matters.

Strong IT support is proactive.

Instead of waiting for tickets, they watch for early warning signs and fix the root cause before staff feel it. They keep systems patched, monitor key services, and bring you recommendations that reduce noise and improve reliability. Not just a scramble after something breaks.

They should also help you meet the expectations of your board (of directors). That includes sensible security controls, clear accountability, and evidence that the basics are in place and being maintained.

You do not need deep technical knowledge to tell if your IT support partner is doing good work. Ask yourself a few simple questions:

- Do they explain options in plain language, without talking down to you?
- Do they understand how a nonprofit operates, not just how technology works?
- Do they bring planning and improvements to the table, or only show up for emergencies?
- Do you feel confident they actually know what is happening across your systems?

Regular review meetings help. They keep priorities clear and give you space to ask questions like:

- “What in our setup concerns you right now?”
- “What should we plan for over the next 12 to 24 months?”
- “Have our backups and recovery steps been tested recently, not just scheduled?”

A strong Chicago-based support partner should understand how local nonprofits operate, including tight budgets, audits, and partner-driven timelines

Warning signs tend to repeat: aging systems that never get refreshed, backups that exist but are never verified, user access that has not been reviewed in a long time, and a general sense that your provider is always reacting instead of leading.

Communication is usually the clearest signal.

> ***If your provider avoids your questions, buries you in jargon, or leaves you unsure what was done and why, you may be depending on the wrong partner. The right IT support should leave you feeling more informed and more in control, not less.***

A clear path to stronger nonprofit IT

Technology touches every part of a nonprofit. How you communicate with donors and partners, how you protect client and program information, how your staff collaborates, and how reliable your operations feel day to day.

You do not need to become the technical expert. You do need confidence that the essentials are covered.

When you keep systems current, protect sensitive data with practical security controls, give your team tools that reduce friction, manage who has access to what, and partner with IT support that understands nonprofit realities and explains things clearly, you avoid most of the problems that drain time and trust.

The real goal is quiet reliability.

You want technology that supports the mission in the background instead of constantly demanding attention, creating workarounds, or introducing new risk. When the fundamentals are right, staff can focus on serving people, building programs, and strengthening relationships, not chasing down tech issues.

For nonprofits in Chicago, dependable IT is not a luxury, it is part of delivering services consistently and protecting trust.

If you want an IT partner that understands nonprofits and helps your board (of directors) feel confident about security, continuity, and day-to-day support, we can help.

Get in touch.

CALL: (312) 985-6810
EMAIL: info@reintivity.com
WEBSITE: www.reintivity.com

REINTIVITY
technology solutions

Serving the Greater Chicago Area