BITRALYNX
SOLUTIONS

FREE EBOOK

9 Technology Mistakes That Put Nonprofits and Law Firms at Risk

A plain guide for leaders who want their staff working and their services running

Bitralynx Solutions
Managed IT, cybersecurity, AI governance, and fractional CIO services for New York nonprofits and law firms
October 2026 | bitralynx.com

About this guide

Most leaders of nonprofits and law firms did not get into this work to manage technology. You got into it to serve people, protect clients, and do good work.

Technology sits quietly in the background. Email works. Files open. The phones ring. Then one day something breaks, and everything stops.

This guide covers nine mistakes we see again and again. None of them come from carelessness. They come from busy people trusting that things are fine. Each chapter tells you what the mistake looks like, why it matters for a nonprofit or a law firm, and what to do this month.

You do not need to be technical to use this guide. We explain terms in plain words the first time they appear. Every chapter ends with three to five steps you can start now.

> How to use this guide. Read a chapter, pick one step, and give it to a person with a date. Small steps that get finished beat big plans that do not.

A note on the numbers. We link every statistic to its source at the end. Where sources disagree or we could only confirm a number in a summary, we say so or use softer words.

CHAPTER 1

Fixing things only when they break

What the mistake looks like

A computer dies, so someone calls for help. The problem is fixed, and everyone moves on. No one asks why it happened or what else might be weak.

Over time, this becomes the whole plan. Updates wait until something fails. No one owns the list of systems. The technology budget is whatever the last emergency cost.

Why it matters for a nonprofit or law firm

Your work depends on being open. A program that cannot check in participants, or an attorney who cannot reach a case file before a deadline, is a real problem for real people.

The cost is large when something serious happens. The 2026 Sophos study of U.S. organizations hit by ransomware (with 100 to 5,000 staff) found an average recovery cost of $2.51 million, not counting any ransom [3]. Your cost may be far smaller, but the lesson holds. Recovery costs more than prevention.

The same study asked why attacks worked. In the U.S., 40% pointed to human error, 38% to a lack of protection, and 37% to a known security gap that was never closed [3]. Those are all things steady attention can reduce.

> Made up example. A small legal aid office has one laptop fail every few months. Each time, a staff member calls someone and gets it fixed. No one notices that every laptop is the same age and none has been updated in a year. The pattern is invisible until the day six fail at once.

What to do this month

1. Name one person who owns technology decisions, even if the work is done by a partner company. Write the name down.
2. Make a one page list of your main systems: email, file storage, case or client software, phones, internet, and who can fix each one.
3. Set a simple yearly technology budget with lines for computers, software, security, backup, training, and a small reserve.
4. Ask for technology input before big choices, such as a new program, a new office, or a new software tool.
5. Put a 30 minute technology review on the calendar every three months.

CHAPTER 2

Backups that no one has ever tested

What the mistake looks like

Someone says, "We have a backup." That may mean a drive in a drawer, a folder on a shared computer, or files in a cloud account. Often no one has ever tried to restore from it.

Backups can fail quietly. They may skip the main server. They may sit on the same network as the original files. They may be old, or the password to open them may be lost.

Why it matters for a nonprofit or law firm

Your records are not replaceable. Case files, client letters, intake records, grant reports, and participant notes may have no second copy.

The 2026 Sophos study found that 60% of U.S. organizations hit by ransomware used backups to get their data back, up from 43% the year before [3]. Backups work when they exist and are ready.

Recovery speed varies a lot. In the same study, 53% were fully recovered in up to a week. But 24% took one to six months [3]. The difference is often preparation.

The U.S. government's guide on ransomware tells organizations to keep offline, encrypted backups of key data and to test them regularly [9]. "Offline" means a copy that an attacker on your network cannot reach.

What to do this month

1. List the data you could not replace. Check that each item is in a backup.
2. Ask: "Is one copy kept somewhere an attacker on our network cannot reach?" If the answer is not a clear yes, fix it first.
3. Pick one folder and one email box. Have someone restore them as a test. Write down how long it took.
4. Make sure two people know where the backup passwords are kept, and that they are stored safely.
5. Repeat the restore test twice a year, and after any big change.

CHAPTER 3

Believing you are too small or too quiet to be a target

What the mistake looks like

"Why would anyone want our files?" It is a fair question, and the answer is not comforting. Most attacks are not aimed at a name. They look for any open door: an old system, a stolen password, a tired employee.

Why it matters for a nonprofit or law firm

Your files are valuable because they are private. Law firms hold client secrets. Nonprofits hold donor details, and many hold health or family information about the people they serve.

Verizon's 2026 breach report found that ransomware was part of 48% of the breaches it studied. It also found that 31% of breaches started by taking advantage of a software weakness, which passed stolen passwords (13%) as the top way in [1].

Attackers also steal data now without locking anything. Sophos found data was stolen in 28% of U.S. attacks where data was also locked [3]. The FBI warned in May 2026 that one group focuses on law firms, steals data quickly, and threatens to post it, usually without using traditional ransomware [4].

The FBI also noted that traditional antivirus is unlikely to flag this kind of attack, because the attackers use normal remote access tools [4]. Antivirus alone is no longer a full answer. Modern tools watch how a computer behaves and can flag odd activity. Those tools are called endpoint detection and response, or EDR, and many are watched by a security team around the clock.

> The question to ask is not "Would anyone want our data?" It is "If our data were taken, what would we have to tell our clients, funders, and regulators?"

What to do this month

1. List where your most private data lives: client files, donor records, health records, HR files.

2. Check that every computer has current protection, and ask whether it is more than basic antivirus.
3. Ask your technology partner who is watching for odd activity outside business hours.
4. Make a list of outside companies that hold your data, such as billing, payroll, or case software. Ask each how they protect it.
5. Decide now who would speak to clients and funders if something went wrong.

CHAPTER 4

Sign in protection that stops at a password or a text code

What the mistake looks like

A password protects the email account. Maybe a text message code is added. Some accounts share one login. A former employee still has access.

Why it matters for a nonprofit or law firm

Email is the key to nearly everything. If someone controls an inbox, they can reset other passwords, read private messages, and send convincing fake requests in your name.

Sophos found that compromised credentials were the root cause in 22% of U.S. ransomware attacks. It also found that 69% said the ransomware event was the same event as their most significant identity attack [3]. In other words, sign in problems and big incidents are often the same story.

Two step sign in, also called multi factor authentication or MFA, is a big help. But not all MFA is equal. Text message and voice codes can be tricked or hijacked. The U.S. cyber agency CISA calls phishing resistant MFA the strongest option and points to security keys and similar standards as the most widely available way to get it [8].

Passkeys are a newer, simpler form of this. A passkey lets you sign in with your face, fingerprint, or device PIN instead of a password or a code. It cannot be handed to a fake website.

If you use Microsoft 365, dates matter. Microsoft says that starting September 1, 2026, passkeys became the default sign in setup for people who were set up for text or voice codes in Microsoft Entra ID (the sign in system behind Microsoft 365). It will stop providing its own text and voice codes for most users on February 1, 2027, and for global administrators and outside users on July 1, 2027. After those dates, people whose only method is a text or voice code must register a passkey to keep signing in. Organizations that truly need text or voice codes can set up a separate phone provider [7]. Plan so that staff are not surprised on a busy Monday morning.

What to do this month

1. Turn on two step sign in for everyone, starting with email, remote access, and administrators.
2. Ask your technology partner which staff still use text or voice codes, and begin moving them to passkeys or an authenticator app.
3. Give every person their own login. No shared accounts.
4. Use a password manager so no one reuses passwords or keeps them on sticky notes.
5. Review who has access. Remove people who left, and limit the number of administrators.

CHAPTER 5

Running old computers and software

What the mistake looks like

Still working, so why replace it? The older office computer, the firewall from several years ago, the case software that has not been updated. Everything feels fine until a weakness is found and no fix is ever released.

Why it matters for a nonprofit or law firm

Budgets are tight, so replacing things feels like a luxury. But old systems are a common way in. Verizon found that taking advantage of software weaknesses was the most common way breaches began in its 2026 report, at 31% [1].

This year there is a clear deadline you may have missed. Microsoft ended support for Windows 10 on October 14, 2025. That means no more regular security fixes or technical

support. Windows 10 computers still turn on and run, but they are not protected the way they were [6].

Microsoft offers paid Extended Security Updates for organizations. The first year costs $61 per computer, the price doubles each year, and the program lasts at most three years. It does not include technical support [6]. Think of it as a short bridge, not a plan.

> Made up example. A counseling nonprofit has 14 office computers. Nine are the same age, and several cannot run the current version of Windows. Replacing nine at once would hurt. Replacing three each quarter, starting with the ones that handle client records, is a plan the board can approve.

What to do this month

1. Make a list of every computer, its age, and its Windows version. Mark any that still run Windows 10.
2. Do the same for firewalls, internet routers, phone systems, and key software.
3. Rank by risk. Machines that handle private records or are used remotely go first.
4. Spread replacement over two budget years instead of one.
5. For anything you must keep a while longer, ask about Extended Security Updates and extra protection around it.

CHAPTER 6

Training that misses today’s scams, including fake IT calls

What the mistake looks like

Training is a short video once a year. It shows an old style phishing email with bad spelling. Staff click through and forget it.

Today's scams do not look like that. Emails are well written. Voice clones can sound like your director. Fake texts look like they came from your bank. And someone may call, claiming to be from your IT team.

Why it matters for a nonprofit or law firm

The FBI issued an alert on May 26, 2026 about a group that pretends to be IT support. Sometimes they email a fake invoice and ask the person to call. Sometimes they call directly and ask the employee to allow a remote session. If that fails, they may send someone to the office to plug in a storage drive, saying a backup is needed [4].

The FBI said this group has consistently targeted U.S. law firms since spring 2023 and has also hit insurance, finance, and healthcare organizations [4].

Artificial intelligence makes scams easier to write. Verizon found that attackers used generative AI to help with about 15% of the attack techniques in its 2026 report [1]. And the FBI's 2025 fraud report shows how costly scams have become. People age 60 and older filed 201,266 complaints and reported $7.7 billion in losses, the highest of any age group [5]. Leaders over 50 are not careless. They are often the ones trusted to approve payments.

Good training now covers three things: urgent requests, calls from "IT," and voices or messages that seem real.

> A simple rule works better than a long lesson. If anyone asks for access, money, or a password, hang up and call back on a number you already know.

What to do this month

1. Tell every person: your IT team will never ask you to install a program or share your screen without a ticket or a pre arranged message. If a call like that comes, hang up and report it.
2. Set a call back rule for any payment change, wire, or gift card request, no matter who seems to be asking.
3. Agree on a code word for urgent money requests that seem to come from leaders.
4. Require that unscheduled visitors claiming to be technicians are escorted and checked with your technology partner first.
5. Run a short 15 minute session every quarter with real, recent examples. Thank people who report suspicious messages. Do not blame people who click.

CHAPTER 7

Assuming cloud services are secure by default

What the mistake looks like

"It's in Microsoft 365, so it's safe." Or Google, or a case management site, or a donor database online. These companies protect their own systems well. But what happens inside your account is mostly up to you.

Why it matters for a nonprofit or law firm

This is called the shared responsibility model. The provider keeps the service running. You decide who gets in, what they can see, what is shared outside, and what is saved elsewhere.

Common problems are not clever hacks. They are old accounts that were never turned off, files shared with "anyone with the link," too many people with administrator rights, and alerts that no one watches.

Cloud storage is also not the same as backup. In SharePoint in Microsoft 365, deleted items are kept for 93 days [13]. After that, a file deleted by mistake, or by an attacker, may be gone. Ransomware can also sync damaged files into the cloud.

The FBI alert noted that attackers copied stolen data to cloud storage such as OneDrive and Google Drive, and used valid accounts to reach email and cloud files [4]. The cloud is part of your front door.

What to do this month

1. Ask for a list of every person with administrator rights. Remove anyone who does not need it.
2. Check sharing settings. Turn off "anyone with the link" for private folders.
3. Turn on alerts for strange sign ins, such as a new country or a new device.
4. Remove accounts for former staff, interns, and volunteers the day they leave.
5. Ask whether your cloud data has a separate backup outside the same account.

CHAPTER 8

Using AI with no rules

What the mistake looks like

Staff are already using AI tools. They paste in a draft letter, a case summary, a grant report, or a participant note to get help. No one decided it was allowed. No one decided it was not. There is no list of approved tools and no rule about what can be entered.

Why it matters for a nonprofit or law firm

AI can save real time, and we are not against it. The risk is data leaving your control. Anything typed into a free or unapproved tool may be stored or used in ways you did not choose.

IBM's 2026 Cost of a Data Breach report reports a 56% increase in AI driven attacks, led by AI deepfake impersonations and AI enabled malware [2]. Good rules and tight access to AI tools are part of the answer.

For law firms there is a professional duty on top. In July 2024 the American Bar Association issued Formal Opinion 512 on lawyers using generative AI. It says the duty of confidentiality applies, and that entering client information into some AI tools may require the client's informed consent. Summaries also say a general line in an engagement letter is not enough [12]. Check your state bar's guidance too.

Nonprofits face their own duties. Funders, partners, and laws may limit how you handle participant information. Health information needs extra care.

What to do this month

1. Ask staff, with no blame, which AI tools they already use. You cannot set rules for what you do not know about.
2. Write a one page AI rule. Cover which tools are approved, what data may never be entered, and that a person checks every result.
3. Say plainly: no client, case, participant, donor, or health details in any tool that is not approved.
4. For law firms, review client consent practices against Opinion 512 and your state bar guidance with your ethics counsel.

5. For each approved tool, ask where data is stored, how long, and whether it is used to train the tool. Review the rule every six months.

CHAPTER 9

No plan for the bad day, and no map of the rules and insurance that apply

What the mistake looks like

If something happened today, who would you call first? Who decides whether to shut systems off? Who tells clients? Many organizations cannot answer in one breath. They also have not read the security questions on their cyber insurance form in years.

Why it matters for a nonprofit or law firm

Time matters on a bad day, and so do legal clocks. Under New York's SHIELD Act, a business must notify affected New York residents within 30 days after discovering a breach, and must also notify the state attorney general, the Department of State, and the State Police. The Department of Financial Services must be told if the business is a covered entity under its cyber rules. The law's list of private information includes medical information, health insurance information, and biometric data [10].

If you handle health information, HIPAA applies today. A proposed update to the HIPAA Security Rule, published in January 2025, has not been finalized as far as we found. The federal regulatory agenda lists final action for July 2027, and dates like this can move [11]. Do not wait. The current rule is the one that counts, and it is worth reviewing with your counsel or compliance lead.

Insurance is also changing. Insurers commonly ask about things like two step sign in, endpoint protection that is watched, and backups that have been tested. Requirements differ by insurer, so check your own policy and application. A wrong answer on a form can cause problems later.

The U.S. cyber agency recommends a simple written incident response plan that is practiced, approved by leadership, and kept in a paper copy [9].

> We do not give legal advice and we cannot guarantee compliance with any law or insurance policy. A written plan, reviewed with your counsel and insurer, is how you prepare.

What to do this month

1. Write a one page plan: who to call first, who decides, who speaks to clients and funders, and how to reach each person if email is down.
2. Add the phone numbers for your technology partner, insurance company, malpractice carrier or funder contacts, and legal counsel. Print a copy.
3. Read your cyber insurance application. Match every answer to what is true today.
4. Know where regulated data lives: health records, client files, financial records. Note which rules apply.
5. Hold a 30 minute talk through. Pick a pretend problem and walk through who does what.

Where do you stand? A one page checklist

Answer each line Yes, Partly, or No. Be honest. No one is grading you.

Ownership and planning

- [ ] We have named one person who owns technology decisions.
- [ ] We have a one page list of our main systems and who supports each.
- [ ] We have a yearly technology budget, including a reserve.

Backups

- [ ] Our key data is backed up automatically.
- [ ] One copy is kept where an attacker on our network could not reach it.
- [ ] We tested a real restore in the last six months.

Who can get in

- [ ] Everyone has their own login, with two step sign in on email.
- [ ] We have started moving from text codes to passkeys or an authenticator app.
- [ ] Former staff and volunteers lose access the day they leave.

Devices and software

- [ ] We know how many computers still run Windows 10.
- [ ] We have a written plan to replace aging computers and firewalls.
- [ ] Our computers have protection that watches for odd behavior, not just basic antivirus.

People

- [ ] Staff know to hang up and call back on a known number if "IT" calls unexpectedly.
- [ ] We have a call back rule for payment changes and money requests.
- [ ] We train staff at least twice a year with current examples.

Cloud and AI

- [ ] We reviewed administrator rights and file sharing settings this year.
- [ ] Our cloud data has a backup outside the same account.
- [ ] We have a written AI rule, and staff know which tools are approved.

Bad day readiness

- [ ] We have a written incident plan with a printed copy and phone numbers.
- [ ] We have checked our insurance application answers against reality.

How to read your score. Count your Yes answers. If you have 15 or more, you are in good shape, and a review will help you keep it that way. If you have 8 to 14, you have a solid base and a few gaps to close. If you have fewer than 8, you are not alone, and the steps in this guide are a good start. This is a guide for conversation, not a formal rating.

Sources

1. Verizon, 2026 Data Breach Investigations Report (data from Nov 1, 2024 to Oct 31, 2025): https://www.verizon.com/business/resources/reports/dbir/
2. IBM, Cost of a Data Breach Report 2026: https://www.ibm.com/reports/data-breach
3. Sophos, The State of Ransomware in the U.S. 2026 (July 2026, 377 U.S. organizations): https://assets.sophos.com/X24WTUEQ/at/tsttpn5wtvfzjw7f4cn89/sophos-state-of-ransomware-in-us-2026.pdf
4. FBI, FLASH-20260526-01, Silent Ransom Group Impersonating IT Personnel through Social Engineering (May 26, 2026): https://www.ic3.gov/CSA/2026/260526.pdf
5. FBI Internet Crime Complaint Center, 2025 Internet Crime Report: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
6. Microsoft Learn, Extended Security Updates (ESU) program for Windows 10: https://learn.microsoft.com/en-us/windows/whats-new/extended-security-updates
7. Microsoft Learn, Passkeys by default and retirement of Microsoft provided SMS and voice authentication (updated Sept 23, 2026): https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sms-voice-retirement
8. CISA, Implementing Phishing Resistant MFA fact sheet: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
9. CISA, #StopRansomware Guide: https://www.cisa.gov/stopransomware/ransomware-guide
10. New York General Business Law Section 899 aa (SHIELD Act, as amended December 2024): https://www.nysenate.gov/legislation/laws/GBS/899-AA
11. Office of Information and Regulatory Affairs (reginfo.gov), Unified Agenda entry, HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information (RIN 0945-AA22): https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=0945-AA22 . Proposed rule: Federal Register, Jan 6, 2025: https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information
12. American Bar Association, Formal Opinion 512, Generative Artificial Intelligence Tools (July 29, 2024): https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf
13. Microsoft Support, Restore deleted items from the site collection recycle bin: https://support.microsoft.com/en-us/office/restore-deleted-items-from-the-site-collection-recycle-bin-5fa924ee-16d7-487b-9a0a-021b9062d14b

NEXT STEP

Talk it through with us

Bitralynx Solutions offers a free 30 minute Technology Readiness Review. It is a conversation, with no access to your systems needed. Bring this guide and your questions. You leave with a short list of what is solid and what to fix first.

Keep your staff working and your services running.

info@bitralynx.com | (516) 855-5353 | bitralynx.com/how-we-start

This guide is general information for nonprofit and law firm leaders. It is not legal advice, a security certification, or a full risk assessment. Facts were checked in October 2026; threats and rules change, so confirm current guidance before you act. Bitralynx Solutions is an IT company, not a law firm.