BITRALYNX
SOLUTIONS

FREE SELF ASSESSMENT

Technology Health Check: A Self Assessment for Nonprofits and Law Firms

Find the gaps before they interrupt the work. Ten sections, 100 points, about 40 minutes.

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

Start here

Your organization runs on technology. Case notes, client files, grant reports, court deadlines, payroll, email. Most of the time it just works, and that is the problem. Gaps stay hidden until the day something stops working.

This guide helps you find those gaps in about 40 minutes. You answer 50 plain questions. You add up a score. You pick your top three fixes. You do not need to be technical.

> **What this is, and what it is not.** This guide helps you spot gaps. It is not a full risk assessment, a security audit, a certification, or legal advice. A high score does not mean you meet any law, rule, contract, or insurance requirement. A low score does not mean you did something wrong. Talk to your own lawyer or compliance advisor about what rules apply to you.

How to use it

Time. Plan for 30 to 45 minutes. Do it in one sitting if you can.

Who should be in the room. Do not do this alone. Bring:

- The person who leads the organization (executive director, managing partner, or office manager)
- Whoever looks after technology day to day, inside or outside your team
- Someone from operations or HR, who knows when people start and leave
- For nonprofits: a program or compliance lead. For law firms: a partner who cares about client confidentiality.

Have these ready if you can. A list of your staff. Your cyber insurance application or policy summary. Your most recent backup report. Do not worry if you cannot find them. That is useful to know.

How to answer. Read each question. Pick one answer, and be honest.

- **Yes** means it is true for everyone and you could show someone. Score 2.

- **Partly** means it is true for some people, some systems, or some of the time. Score 1.
- **No** means it is not true. Score 0.
- **Not sure** counts as No. If you do not know, that is the finding.

Questions marked with a star (★) matter most. If you answer No to a starred question, add it to your fix list even if your section score is good.

Each section has 5 questions, so each section is worth up to 10 points. There are 10 sections, so the total is 100.

SECTION 1

Sign in and accounts

Why it matters. Stolen or guessed passwords are one of the most common ways attackers get in. Verizon's 2026 Data Breach Investigations Report found that stolen credentials started 13 percent of the breaches it studied, and that a human element, such as a click or a reused password, was present in 62 percent [1]. Sophos found compromised credentials behind 22 percent of ransomware attacks in its 2026 U.S. survey, and 69 percent said the ransomware event was the same event as their most significant identity attack [2]. Strong sign in protects email, files, and client records all at once.

#	Question	Yes	Partly	No
1.1 ★	Does every person use two step sign in (also called MFA, where you confirm with a second item like an app or a key) on email and file storage?	☐	☐	☐
1.2 ★	Do the most powerful accounts (administrators, finance, partners, executives) use the strongest kind of two step sign in, such as passkeys or security keys, not just text messages?	☐	☐	☐
1.3	Does everyone use a password manager, so no one reuses passwords or keeps them on sticky notes or in a spreadsheet?	☐	☐	☐
1.4 ★	When someone leaves or changes roles, is all of their access removed or changed on their last day?	☐	☐	☐

#	Question	Yes	Partly	No
1.5	Do you review who has administrator access, and who can see sensitive folders, at least twice a year?	☐	☐	☐

Plain note on text message codes. Text and phone call codes are better than nothing. But they can be tricked or intercepted more easily than app based or key based methods. A *passkey* is a sign in method that uses your device, like a fingerprint or face unlock, instead of a password. The U.S. cyber agency CISA calls this family of methods "phishing resistant" [3]. Also, Microsoft is retiring its own text and voice call sign in codes for Microsoft Entra accounts. Passkeys became the default for people set up for those codes on September 1, 2026. Text and voice delivery ends February 1, 2027 for most users, and July 1, 2027 for global administrators and outside users. After those dates, people whose only method is a text or voice code must register a passkey to keep signing in [4]. If you use Microsoft 365, ask whoever manages it to check your plan now.

First fixes

1. Turn on two step sign in for every account, starting with email. Do administrators first.
2. Write a one page "leaver checklist" and use it every time. Name who is responsible.
3. Move your administrators and executives to passkeys or security keys.

Section 1 score: ____ / 10

SECTION 2

Devices and updates

Why it matters. Computers, laptops, phones, and tablets hold your data and open the door to your systems. Old or unpatched devices are easy to attack. Verizon's 2026 report found that software weaknesses are now the most common way breaches begin, at 31 percent [5]. Sophos found a lower share in its 2026 U.S. ransomware survey, 16 percent, down from 27 percent the year before [2]. Studies count differently, but both show that unpatched devices matter.

Windows 10 reached end of support on October 14, 2025. That means regular security updates stopped for most computers still running it. Microsoft has a paid and limited program called Extended Security Updates, but its consumer version cannot be used for business setups, and the consumer program now runs to October 12, 2027 [6]. Treat any extended update plan as a short bridge, not a plan. Replace or upgrade Windows 10 computers.

#	Question	Yes	Partly	No
2.1 ★	Are all computers running a version of Windows or macOS that still gets security updates (no Windows 10)?	☐	☐	☐
2.2	Do updates install automatically, and does someone check that they actually did?	☐	☐	☐
2.3 ★	Do all computers have protection that watches for and responds to threats (often called EDR, not just basic antivirus), with someone who looks at the alerts?	☐	☐	☐
2.4	Are laptops and phones encrypted (scrambled so a lost device cannot be read) and set to lock after a short time?	☐	☐	☐
2.5	Do you keep a list of every device, who uses it, and when it should be replaced?	☐	☐	☐

First fixes

1. Count your Windows 10 computers. Make a replacement list with dates.
2. Turn on disk encryption on every laptop, and a screen lock on every phone.
3. Make one person responsible for checking that updates and protection are working.

Section 2 score: ____ / 10

SECTION 3

Email and scam defense

Why it matters. Email is where most scams begin. Scammers now use AI to write cleaner messages and even to copy voices. In 2025 the FBI warned about text messages and AI made voice messages pretending to be senior officials, built to earn trust and then steal logins [7]. The FBI's Internet Crime Complaint Center reported record losses of about $20.9 billion across all kinds of cybercrime for 2025, from more than one million complaints [8]. Nonprofits and law firms handle money and wire instructions, which makes them targets for fake payment requests.

#	Question	Yes	Partly	No
3.1 ★	Does your email filter block dangerous links and attachments, and warn about messages from outside your organization?	☐	☐	☐
3.2 ★	Is there a rule that any change to payment details, wire instructions, or a bank account is confirmed by calling a known phone number, never the number in the message?	☐	☐	☐
3.3	Are your email domain protections (called SPF, DKIM, and DMARC, which help stop people from faking your email address) set up and checked?	☐	☐	☐
3.4	Does your team know that a voice or video call can now be faked, and do you have a way to verify a surprise request from a leader or a client?	☐	☐	☐
3.5	Can staff report a suspicious message with one click or one phone call, and do they hear back?	☐	☐	☐

First fixes

1. Adopt a "call back on a known number" rule for money and bank details. Write it down.
2. Ask whoever manages your email to confirm filtering and domain protections are on.
3. Pick a simple private phrase or check step for urgent requests from leaders.

Section 3 score: ____ / 10

SECTION 4

Backups and recovery

Why it matters. A backup is a copy you can restore from. Many groups think syncing files to the cloud is a backup. It is not. If files are deleted or locked by an attacker, the change can sync everywhere. CISA advises keeping offline, encrypted backups of critical data and testing them regularly [9]. Sophos found that 60 percent of U.S. organizations hit by ransomware used backups to recover their data, up from 43 percent the year before. It also found that the average cost to recover was about $2.51 million, not counting any ransom [2]. Those are survey figures from organizations with 100 to 5,000 staff that were hit by ransomware, so yours may be smaller. They show why backups and testing matter.

#	Question	Yes	Partly	No
4.1 ★	Are your important systems and files backed up automatically every day, including email, shared files, and your case or client database?	☐	☐	☐
4.2 ★	Is at least one copy kept separate from your main network, so an attacker who gets in cannot delete it?	☐	☐	☐
4.3 ★	Have you actually restored files from backup in the last 6 months, and written down how long it took?	☐	☐	☐
4.4	Does someone get an alert if a backup fails?	☐	☐	☐
4.5	Do you know how long you could go without your key systems, and have leaders agreed that it is acceptable?	☐	☐	☐

First fixes

1. Ask for a restore test this month. Pick five real files and one full folder.
2. Make sure one backup copy is offline or cannot be changed by regular accounts.
3. Write down your top five systems and how long you can live without each.

Section 4 score: ____ / 10

SECTION 5

Network and Wi Fi

Why it matters. Your network connects every device, phone system, and cloud tool. Home grade equipment and old settings are common in small offices. Guest devices, visitors, and clients should not share a network with your files.

#	Question	Yes	Partly	No
5.1 ★	Is your firewall (the gate between your office and the internet) business grade, supported by its maker, and updated on a schedule?	☐	☐	☐
5.2	Is guest Wi Fi kept separate from the network your staff use?	☐	☐	☐
5.3	Does the office Wi Fi use a strong, current setting (WPA2 or WPA3) and a password that changes when staff leave?	☐	☐	☐
5.4	Do people working from home or from client sites connect to your systems in a secure way, using approved devices?	☐	☐	☐
5.5	Has someone qualified reviewed your network settings in the last 12 months, and do you have a simple diagram or list of what is connected?	☐	☐	☐

First fixes

1. Find out the age and support status of your firewall and internet router.
2. Set up a separate guest Wi Fi if you do not have one.
3. Put a yearly network review on the calendar.

Section 5 score: ____ / 10

SECTION 6

Vendors and apps

Why it matters. Your data lives in many tools and with many outside companies: your database, payroll, case management, donor system, phone provider, and IT provider. Verizon's 2026 report found that outside parties were involved in 48 percent of the breaches it analyzed, up 60 percent from the year before [5]. You are still responsible for the data you hand to a vendor.

#	Question	Yes	Partly	No
6.1 ★	Do you have one list of every app and outside provider that holds your data, with an owner for each?	☐	☐	☐
6.2	Do you know which vendors can reach into your systems remotely, and can you turn that access off?	☐	☐	☐
6.3	Before you sign up for a new tool, does someone check how it protects data and where the data goes?	☐	☐	☐
6.4	Are free or personal accounts (personal email, free file sharing) kept out of work?	☐	☐	☐
6.5	Do you review vendor contracts each year for what happens to your data if you leave or if they have a breach?	☐	☐	☐

First fixes

1. Build the list in a simple spreadsheet. Ask each department what they use.
2. Close any vendor access that no one can explain.
3. Add three questions to your buying process: Where is our data, who can see it, and can we get it back?

Section 6 score: ____ / 10

SECTION 7

AI use

Why it matters. Your staff are probably already using AI tools, with or without your say. That can help the work. It can also put private client or participant information into a tool you do not control. Anything typed into an unapproved tool can leave your control. IBM's 2026 breach report found a 56 percent rise in AI driven attacks, led by AI deepfake impersonations and AI enabled malware [10]. For lawyers, the American Bar Association's Formal Opinion 512 (July 2024) says existing duties on competence, confidentiality, supervision, and honesty with the court apply to AI tools. It also says informed client consent is needed before putting client information into some tools, and that a standard line in an engagement letter is not enough [11]. Ask your own counsel how your state's rules apply. Nonprofits that serve health, housing, or youth clients face similar trust questions.

#	Question	Yes	Partly	No
7.1 ★	Do you have a short written rule on which AI tools staff may use, and what they must never paste into them (client names, case details, health information, donor data)?	☐	☐	☐
7.2	Do you know which AI tools people are using today, including free ones on personal accounts?	☐	☐	☐
7.3 ★	Does a person check AI output before it goes to a client, a funder, or a court?	☐	☐	☐
7.4	Have you read the privacy terms of the AI tools you approve, including whether your inputs are used to train the tool?	☐	☐	☐
7.5	Do your leaders know who is accountable for AI decisions, and is there a place to ask questions?	☐	☐	☐

First fixes

1. Write a one page AI use rule. Say what is allowed, what is not, and who to ask.
2. Offer an approved tool so staff do not hunt for their own.
3. Make "a human reviews it" a standing step for anything that leaves the building.

Section 7 score: ____ / 10

SECTION 8

Staff habits and training

Why it matters. Good tools fail when people are rushed or unsure. Attackers also call and pretend to be IT staff. CISA's advisory on a group called Scattered Spider describes callers who talk help desks into resetting passwords and MFA [12]. Short, regular training and a no blame culture make staff more likely to speak up fast.

#	Question	Yes	Partly	No
8.1 ★	Does every new person get a short security briefing in their first week, and a refresher at least once a year?	☐	☐	☐
8.2	Do staff practice with short, realistic examples (fake emails, fake calls) a few times a year?	☐	☐	☐
8.3 ★	Is there a rule for how your help desk or IT provider confirms who is calling before resetting a password or sign in method?	☐	☐	☐
8.4	Do staff feel safe saying "I think I clicked something," without fear of blame?	☐	☐	☐
8.5	Do volunteers, board members, contractors, and interns follow the same basic rules as staff?	☐	☐	☐

First fixes

1. Add a 20 minute security briefing to your first week checklist.
2. Agree on a script for identity checks before any password or MFA reset.
3. Tell staff, in writing, that quick reporting is always welcome.

Section 8 score: ____ / 10

SECTION 9

Incident readiness

Why it matters. When something goes wrong, the first hour is confusing. A short plan saves time and stress. CISA advises organizations to create, keep, and practice a basic incident response plan and keep a paper copy, in case your systems are down [9]. Also know your reporting duties. New York law requires notice to affected New York residents in the most expedient time possible and within 30 days after discovery of a breach of private information, and notice to certain state offices. The definition of private information now includes medical and health insurance information [13]. If you handle health records, other rules may apply.

> **HIPAA update.** In January 2025, the U.S. Department of Health and Human Services proposed a major update to the HIPAA Security Rule. As of our last check, we found no final rule, and the federal regulatory agenda lists final action for July 2027. Dates like that can move [14]. The current Security Rule still applies today. If you are a covered entity or a business associate, ask your compliance advisor what you need now.

#	Question	Yes	Partly	No
9.1 ★	Is there a written plan that names who does what in the first hour, with phone numbers kept on paper and off your network?	☐	☐	☐
9.2 ★	Do you know who you would call first: your IT provider, your lawyer, your insurer, and your cyber insurance claims line?	☐	☐	☐
9.3	Do you know which laws, contracts, or funder rules could require you to report an incident, and how fast?	☐	☐	☐
9.4	Have leaders talked through one made up scenario, like a locked file server or a stolen laptop, in the last 12 months?	☐	☐	☐
9.5	Do you know what your cyber insurance covers, what it asks of you, and who must be called first?	☐	☐	☐

First fixes

1. Print a one page contact sheet and give a copy to each leader.
2. Hold a 45 minute tabletop talk: "It is Monday morning and no one can open files. What do we do?"
3. Read your cyber insurance summary. Note what the carrier says you must have in place.

Section 9 score: ____ / 10

SECTION 10

Records you can show others

Why it matters. Funders, auditors, insurers, boards, and clients increasingly ask for proof, not promises. Being able to show a short set of records builds trust and saves time at renewal and audit. Insurers commonly ask about things like two step sign in, tested backups, and incident plans. Each policy differs, so read yours.

#	Question	Yes	Partly	No
10.1 ★	Could you hand someone a current list of devices, users, and apps within a day?	☐	☐	☐
10.2	Do you keep written technology policies (acceptable use, AI use, passwords, remote work, leaver steps), reviewed this year?	☐	☐	☐
10.3	Do you keep proof that key controls work, such as backup restore tests, update reports, and training dates?	☐	☐	☐
10.4	Is there a yearly technology plan and budget that leaders and the board have seen?	☐	☐	☐
10.5	Could you answer a funder, insurer, or client security questionnaire without scrambling?	☐	☐	☐

First fixes

1. Start a folder called "Technology Evidence." Drop in restore tests, training records, and policies as you go.

2. Put a short technology update on your board or partner meeting agenda once a quarter.
3. Keep a simple answer sheet for common security questionnaires.

Section 10 score: ____ / 10

Your score

Step 1. Record your section scores

Section	Score (0 to 10)
1. Sign in and accounts	
2. Devices and updates	
3. Email and scam defense	
4. Backups and recovery	
5. Network and Wi Fi	
6. Vendors and apps	
7. AI use	
8. Staff habits and training	
9. Incident readiness	
10. Records you can show others	
Total	**____ / 100**

Points per answer: Yes = 2. Partly = 1. No or Not sure = 0.

Step 2. Read each section score

- **8 to 10:** Strong. Keep it up and recheck once a year.
- **5 to 7:** Gaps. Work on this section within the next few months.
- **0 to 4:** Priority. Start here.

Step 3. Read your total

80 to 100: Strong footing. Your basics are in place and you can show it. Keep checking once or twice a year, and watch for changes in tools, laws, and threats.

60 to 79: Solid base with gaps. You are doing many things right, but some gaps could slow you down in a bad week. Pick your top three fixes and schedule them this quarter.

40 to 59: Real gaps. Several important protections are missing or unproven. Staff and services could be interrupted. Make a plan with dates, and get outside help if you do not have the time or skills in house.

0 to 39: Urgent attention. Important basics are missing. This is not a judgment. Many organizations start here, especially if technology was set up years ago and never reviewed. Start with sign in, backups, and Windows 10 computers, and talk with a technology partner soon.

> **Star check.** Count how many starred (★) questions you answered No or Not sure. If it is more than three, treat your result as one band lower than your score says. A good total can hide one serious gap.

How to read your score honestly

This is a self check. It shows what you know and believe today. It does not test your systems. It will not find things no one in the room knows about. It does not tell you whether you meet a law, funder rule, contract, or insurance requirement. For that you need a proper review and, where needed, your own legal or compliance advisor.

Your top 3 fixes

Choose the three fixes that would reduce the most risk for the least effort. Start with any starred No answers and any section scored 0 to 4.

	Fix	Who owns it	Due date	Needs outside help? (Y/N)
1				
2				
3				

Next review date: _____

People who signed off on this plan: _____

> **Small steps count.** Three finished fixes beat a long list that never gets done. Come back in 90 days and score again.

Sources

1. Verizon, 2026 Data Breach Investigations Report and Executive Summary (credential abuse 13 percent of initial access; vulnerability exploitation 31 percent; human element 62 percent; third party involvement 48 percent). https://www.verizon.com/business/resources/reports/dbir/ and https://www.verizon.com/business/resources/executivebriefs/2026-dbir-executive-summary.pdf
2. Sophos, The State of Ransomware in the U.S. 2026 (July 2026; 377 U.S. organizations with 100 to 5,000 staff, all hit by ransomware; compromised credentials 22 percent; exploited vulnerabilities 16 percent; backups used 60 percent; average recovery cost $2.51 million). https://assets.sophos.com/X24WTUEQ/at/tsttpn5wtvfzjw7f4cn89/sophos-state-of-ransomware-in-us-2026.pdf
3. CISA, Implementing Phishing Resistant MFA fact sheet. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
4. Microsoft Learn, Passkeys by default and retirement of Microsoft provided SMS and voice authentication (page dated September 23, 2026). https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sms-voice-retirement
5. Verizon 2026 DBIR (same report as source 1; vulnerability exploitation 31 percent, third party involvement 48 percent, up 60 percent). https://www.verizon.com/business/resources/executivebriefs/2026-dbir-executive-summary.pdf
6. Microsoft, Windows 10 Extended Security Updates page (end of support Oct 14, 2025; consumer ESU through Oct 12, 2027; consumer program not for business setups). https://www.microsoft.com/en-US/windows/extended-security-updates
7. FBI IC3 Public Service Announcement, May 15, 2025, AI voice and text impersonation campaign. https://www.ic3.gov/PSA/2025/PSA250515
8. FBI Internet Crime Complaint Center, 2025 Internet Crime Report ($20.877 billion in reported losses; 1,008,597 complaints). https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
9. CISA, #StopRansomware Guide (offline encrypted backups, tested restores, incident response plan with a hard copy). https://www.cisa.gov/stopransomware/ransomware-guide
10. IBM, Cost of a Data Breach Report 2026 (56 percent increase in AI driven attacks). https://www.ibm.com/reports/data-breach
11. 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 and news release: https://www.americanbar.org/news/abanews/aba-news-archives/2024/07/aba-issues-guidance-lawyers-use-ai-tools/
12. CISA and FBI, Advisory AA23-320A, Scattered Spider (updated 2025). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
13. New York General Business Law section 899-aa (30 day notice; regulators to notify; private information includes medical and health insurance information). https://www.nysenate.gov/legislation/laws/GBS/899-AA
14. HHS HIPAA Security Rule proposed rule, Federal Register, January 6, 2025: https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information and Unified Agenda entry (RIN 0945-AA22): https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=0945-AA22
15. NIST, Cybersecurity Framework 2.0 Small Business Quick Start Guide (SP 1300), suggested further reading. https://csrc.nist.gov/pubs/sp/1300/final

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.