Take Charge of Your Cybersecurity

The Financial Advisor's Cyber Readiness Checklist

The 15 things a regulator, an insurer, or a client may ask you to prove. And a calm way to know where your firm stands.

From H2Cyber. Veteran owned. Built by a 30-year cybersecurity practitioner.

Why this checklist

At some point, someone asks a small firm to show its cybersecurity posture. It is a regulator with an exam notice, an insurer with a renewal application, or a client doing their own due diligence. The firms that handle this calmly are the ones who already knew where they stood.

This is the short version of what they ask about. Fifteen plain-English checkpoints, grouped the way an owner thinks, not the way a framework is written. You do not need to be technical to use it. For each item, check the box if you can say yes with confidence. If you are not sure, that is the most useful answer of all, because now you know where to look.

This is not the whole picture. The full assessment covers 56 controls and gives you a letter grade. But these 15 are the ones that come up first, and they are a good place to start.

Two of them, multi-factor authentication and endpoint protection, are flagged as items insurers often require. On a cyber insurance application, missing either one is frequently an automatic disqualifier.

The checklist

1. Logins and access

- [ ] **Multi-factor authentication is on.** Email and anything that holds client data ask for a second step at login, not just a password.

  Insurers often require this.

- [ ] **Everyone has their own login.** No shared accounts and no shared passwords.
- [ ] **Access ends when someone leaves.** When a person departs, their access is shut off the same day.
- [ ] **Passwords are long and unique.** Ideally kept in a password manager, not on a sticky note or reused across sites.

2. Email

- [ ] **Your email plan actually includes security.** Many firms pay for mail and assume protection comes with it. It often does not (see the callout below).
- [ ] **Your email is protected against spoofing and phishing.** Messages that impersonate you or your clients get caught, not delivered.

> **The one most firms miss.**
>
> A lot of firms run on Microsoft 365 and assume that covers them. The cheaper plans, Business Basic and Standard at around $4 to $6 per user a month, include almost no security. The plan that actually protects your email and your devices is Business Premium, around $23 per user a month. Most firms are on the cheaper one and were never told the difference. This single line item is the most common gap we find, and it is a money question, not a fear one.

3. Devices

- [ ] **Every device that touches client data is protected.** Each laptop and phone runs endpoint protection, often called EDR, that watches for and stops malicious activity.

  Insurers often require this.

- [ ] **Laptops and phones are encrypted.** A lost or stolen device is an inconvenience, not a client-data breach.
- [ ] **Updates install promptly.** Operating systems and applications keep themselves current, so known holes get closed.

4. Data and backups

- [ ] **Client data is backed up automatically.** You are not relying on someone remembering to do it.
- [ ] **You have actually restored from a backup.** A backup you have never tested is a hope, not a plan. You have confirmed you can get your data back.

5. Policy and people

- [ ] **You have a written information security policy.** Examiners ask for this one by name. It does not need to be long, it needs to exist and reflect what you actually do.
- [ ] **Your team can spot a phishing email.** The people in your firm know what a suspicious message looks like and what to do with it.
- [ ] **You have a simple incident response plan.** If something happens, you know who to call and what the first steps are, before you need to.
- [ ] **You know which vendors can see your client data.** You have a short list of the outside services and people with access, so there are no surprises.

How did you do?

There is no failing grade here. This is a starting point, not a verdict.

You checked most of them.

You are in better shape than most small firms. The assessment confirms it, fills in the rest of the 56 controls, and gives you a grade and a seal you can show.

You checked about half.

That is normal, and it is exactly the firm H2Cyber was built for. The basics that matter most are usually a week or two of focused work, not a year-long project.

You were not sure on several.

That is the most useful result of all. You now know where to look, and the assessment turns "not sure" into a clear, prioritized plan.

See where your firm really stands

This checklist is the short list. The H2Cyber assessment is the full picture: 56 plain-English controls, a letter grade from A to F, and a prioritized plan that tells you what to fix first. It is free to take, there is no credit card, and the grade is yours to keep.

A cybersecurity practitioner built it specifically for small firms that do not have an in-house security team. The tool does the expert work. You answer the questions.

Take the assessment and get your grade, free, at h2cyber.com.

And when a regulator, an insurer, or a client asks how you are managing cyber risk, you will have a real answer, and a report to back it up. H2Cyber reduces your risk and the damage if something does happen. No one can promise to prevent every incident, but you can absolutely lower the odds and the cost.