Six things to have in place by next month

Hand this to whoever runs your IT, and ask for a yes or no on each line.

1 Callback rule for IT and payment requests ☐

Your IT team will never ask you to sign in or approve a prompt over the phone. If someone does, hang up and call back on a number you already have.

Why it matters: In September, fake help desk calls were used to steal Microsoft 365 data from executives.

2 Phishing-resistant sign-in for leaders ☐

Passkeys or security keys for owners and anyone who moves money, plus rules that block sign-ins from devices you don't own.

Why it matters: A normal multi-factor prompt can be approved for the wrong person.

3 Payment changes confirmed by phone, by two people ☐

New bank or routing details for any vendor get a call to a number you already had, plus a second person's approval.

Why it matters: Business email compromise cost U.S. businesses over $3 billion in 2025.

4 File access trimmed ☐

One account shouldn't be able to open every SharePoint and OneDrive folder in the company.

Why it matters: Stolen sign-ins are used to copy files in bulk, followed by a demand for payment.

5 Internet-facing devices listed and patched within days ☐

Your firewall, VPN and remote access gear are written down with make, model and version, and a named person patches critical flaws fast.

Why it matters: Two Citrix NetScaler flaws were attacked for weeks before a patch existed.

6 Unsupported gear on a replacement list with a date ☐

Anything the maker stopped updating gets a replacement date, starting with what faces the internet.

Why it matters: Older NetScaler versions got no fix at all this time.

Where to start, by industry

Law firms: Start with items 1 and 4. Client files and wire instructions for closings are the target.

CPAs and finance: Start with items 2 and 3. Whoever touches client money or tax data gets the strongest sign-in.

Construction and engineering: Start with items 1 and 3. Executives were named targets, and vendor payment changes happen constantly.

Sources: FBI IC3 2025 Internet Crime Report (April 2026); Arctic Wolf, PREY-0058 (September 2026); CISA and Citrix NetScaler alert (September 27, 2026); CenterPoint Energy statement (September 16, 2026).