CLOUD CONFIGURATION RISKS

Your data is only as secure as your settings.

The Vulnerability Gap

As firms migrate to cloud-based tax software and document portals, the greatest risk isn't the cloud provider—it's **misconfiguration**. One "Public" setting on a folder can expose thousands of taxpayer IDs to the internet.

Top 3 Cloud Blind Spots

1. **Over-Permissioning:** Staff members having access to files they don't need for their specific role.
2. **Legacy MFA:** Relying on SMS codes (which are easily intercepted) rather than app-based authenticators or hardware keys.
3. **Shadow IT:** Staff using personal Dropbox or Google Drive accounts to move client files because "it's faster."

The CardinalsByte Checklist

Hardening Your Cloud Environment

- Enable **Conditional Access** (e.g., logins only allowed from the US).
- Implement **Data Loss Prevention (DLP)** to block the emailing of SSNs.
- Audit your third-party app permissions monthly.

CardinalsByte

Cybersecurity Compliance & Risk for:
Small Business, CPAs, Tax Professionals, Bookkeepers and Accountants

www.cardinalsbytes.com