SME Digital Advisor

Plain-English advice on digital risk

RISKS · CARDS

Risk Flashcards

All 25 plain-English digital risks. One topic per card.

Reference site for SME owners. Free. No sign-up.

Companion to andrewreaassociates.com

smedigitaladvisor.co.uk

RISK 01 OF 25 · BUSINESS-CRITICAL SYSTEM AUDIT

Do you know what technology your business actually depends on?

Many SMEs rely on hidden systems: old databases, spreadsheets, Access files, internal websites, macros, scripts, file shares, and tools built years ago by someone who has since left.

What you can do:
1. Print this question and stick it on the wall: *"If our IT person quit on Friday, what's the first thing that would break by Tuesday?"* Ask three people separately.

2. Open your last bank statement. Every IT-related direct debit you can't match to a system is a system you didn't know you depend on.

3. Open Microsoft 365 admin → **Active users**. Cross-check every account against payroll.

RISK 02 OF 25 · HIDDEN BUSINESS RISK IN LEGACY SYSTEMS

Could one old system stop your business trading?

A lot of SMEs have systems that "just work" — until they don't.

What you can do:
1. Walk the office. Find the "if this PC dies, we stop" machine. Photograph the serial-number sticker.

2. List the five systems you'd notice in under an hour if they went down. Next to each: when was it last patched?

3. Check the operating system on your most critical server. Windows Server 2012 R2 / 2016 / earlier are out of support.

RISK 03 OF 25 · LEGACY TECHNOLOGY MODERNISATION

Are you relying on software nobody understands anymore?

Long-established SMEs often have systems that scare people — because no one wants to be the one who touches them.

What you can do:
1. Open the app. **Help** → **About**. Note the version. Now Google: *"[product name] [version] end of life."*

2. Find the original developer or vendor (LinkedIn is fine). One short message: *"Do you still support this?"*

3. If the app uses a database, look for a default `sa`, `admin`, or `root` account with a weak password.

RISK 04 OF 25 · SPREADSHEET RISK REVIEW

Are old spreadsheets quietly running your business?

Spreadsheets are useful, but they often become unofficial business systems — without owners, without testing, without backup.

What you can do:
1. Open Documents/Desktop. Sort by "Date modified." Anything called *Master*, *Live*, *FINAL_v3_real* that's been touched today is probably running something.

2. For each, ask: *"If this file vanished now, how long would it take to rebuild?"*

3. Use **Review** → **Protect Sheet** on at least the formula cells. Costs nothing.

RISK 05 OF 25 · ACCESS CONTROL AND ACCOUNTABILITY

Are ex-employees or old suppliers still able to access your systems?

Many companies have employees, suppliers, consultants, or old accounts with far more access than they need — sometimes long after they've left.

What you can do:
1. Microsoft 365: **Admin Center** → **Users** → **Active users**. Cross-check every name against payroll.

2. Look at your most important shared inboxes. Who has “send as” or delegate access?

3. Send one email to every external supplier with access: *“Tell me which accounts your team has, and when each was last used.”*

RISK 06 OF 25 · PASSWORD AND ACCOUNT SAFETY

Could one weak password expose your company?

This isn't about technical password policy. It's about whether one weak login could unlock the whole business.

What you can do:
1. Turn on MFA for every admin account in Microsoft 365 / Google Workspace. **Admins only, today.**

2. Run your director-level email addresses through haveibeenpwned.com.

3. Get a real password manager — 1Password, Bitwarden, or Dashlane all have business tiers under £5/user/month.

RISK 07 OF 25 · PROTECTING BUSINESS DATA

Could a simple mistake delete or corrupt important data?

This is the heart of cybersecurity for most SMEs — and it isn't always about hackers.

What you can do:
1. Turn on **Version History** on shared folders. Restoring becomes one click.

2. On accounts and finance folders, restrict the **Delete** permission to two named people.

3. Check your Microsoft 365 retention policy. Default is around 30 days; longer if your business needs it.

RISK 08 OF 25 · DATA PROTECTION AND COMPLIANCE READINESS

Do you know where your sensitive data is stored?

This matters because it affects fines, insurance, client contracts, and reputation.

What you can do:
1. Draw four boxes on paper: *Customer*, *Employee*, *Financial*, *Supplier*. For each: where it lives, who reads, who deletes.

2. Look at three random staff laptops. Customer lists on a laptop are data leaving the building each evening.

3. Look at your office Wi-Fi router. List every connected device.

RISK 09 OF 25 · MANUFACTURING SYSTEM RESILIENCE

Could one old PC stop your production line?

For manufacturers and operational businesses, the real concern is downtime, missed orders, production errors.

What you can do:
1. Find every Windows PC on the line. Note the OS. Anything older than Windows 10 / Server 2019 is a problem.

2. Ask the line manager: *"Which of these, if it died, stops production?"*

3. Ask: "Are factory systems on the same network as the office?" If you don't know, the answer is almost always "yes."

RISK 10 OF 25 · BACKUP AND RECOVERY CONFIDENCE

Are your backups real, or just assumed?

Many SMEs believe they have backups, but no one has ever tested restoring from them.

What you can do:
1. Pick a non-critical file. **Delete it.** Try to restore. Time how long it takes.

2. Email your IT supplier: *"Send me the dated screenshot of the most recent successful end-to-end restore test."*

3. Check whether your Microsoft 365 data is in any backup. Microsoft's shared-responsibility model says it's your job.

RISK 11 OF 25 · CYBER INCIDENT READINESS

Would you survive a ransomware attack?

Owners need to know the likely impact and who picks up the phone.

What you can do:
1. Write a one-page "if everything is down" plan. Put it in three places that are *not* on the network.

2. Add to your phone: IT supplier's emergency number, cyber insurer's claim line, ICO (0303 123 1113).

3. Check your cyber insurance — most include an incident response provider. Find their hotline.

RISK 12 OF 25 · MONITORING AND EARLY WARNING SYSTEMS

Would you know quickly if something was wrong?

Many SMEs only discover problems after customers complain or data has already gone.

What you can do:
1. Sign up to UptimeRobot (free tier).

2. Add calendar reminders for domain expiry, SSL expiry, IT contract end date — with 90-day warnings.

3. Ask your IT supplier: *"Where do alerts go, and who reads them?"*

RISK 13 OF 25 · INDEPENDENT REVIEW OF IT SUPPLIERS

Are you paying for IT support but still carrying serious risk?

An SME can believe “the IT company has it covered” when in reality no one is challenging the quality.

What you can do:
1. Reread the SLA. Search for **security** and **backup**. If they aren't there, that work isn't their job.

2. Email your supplier: *“What three risks are you actively managing for me?”*

3. Find out who legally owns your **domain name**, **DNS**, and **master Microsoft 365 / Google admin**.

RISK 14 OF 25 · STAFF-BUILT SYSTEMS AND AI-CREATED TOOLS

Are staff building business-critical tools without you knowing?

AI and low-code make it easy for non-technical staff to create apps the business now depends on.

What you can do:
1. Microsoft 365 admin centre → **Reports** → **Power Platform Apps** and SharePoint sites created in the last year.

2. Ask three staff: *“What tool have you built this year that you think the team now relies on?”*

3. Start a **tools register**. Name, owner, what it does, what data it touches, what happens if the owner leaves.

RISK 15 OF 25 · SAFE AND PRODUCTIVE AI ADOPTION

Is AI creating hidden risk inside your business?

AI is useful. Unmanaged AI use creates data, security, legal, and quality risks — sometimes all at once.

What you can do:
1. Send one email to all staff: *“What AI tools, what data?”*

2. For each AI tool, check its **data retention** setting. Free tiers usually *do* train on your input.

3. Write a single A4 page: *“What's OK and not OK to put into AI.”*

RISK 16 OF 25 · WEBSITE AND PORTAL RISK REVIEW

Are your customer portals and websites safe?

A hacked website or insecure customer portal causes lost trust, lost sales, and legal problems.

What you can do:
1. Open your website. Click the padlock. Check certificate name, issuer, expiry.

2. Paste your URL into securityheaders.com. Aim for at least a **B grade**.

3. List every domain your business owns: registrar, expiry, login owner.

RISK 17 OF 25 · CHANGE CONTROL FOR GROWING BUSINESSES

Are changes being made safely, or just made?

Many SMEs make changes informally with no record and no way back.

What you can do:
1. Ask your IT supplier for “the last five changes you made.”

2. On business-critical spreadsheets, turn on **Version History**.

3. Set a 24-hour rule: *no live change to a business-critical system goes in on a Friday afternoon.*

RISK 18 OF 25 · CUSTOMER TRUST AND SECURITY ASSURANCE

Can you prove to customers that their data is safe?

Larger customers increasingly ask SMEs for evidence of cybersecurity and data protection.

What you can do:
1. Look up Cyber Essentials. The questionnaire is free.

2. Find your most demanding customer's data-protection clause. Could you evidence it tomorrow?

3. List the policies you could produce in five minutes: data protection, acceptable use, password, incident response, AI.

RISK 19 OF 25 · IT SPEND AND RISK PRIORITISATION

Is your IT spend actually reducing risk?

Many SMEs spend plenty on IT but still have serious gaps.

What you can do:
1. Print your last three IT invoices. Beside each line item, write: *what business risk does this reduce?*

2. Ask your IT supplier for a categorised invoice.

3. Look at your IT contract renewal date. Within 90 days = peak negotiating leverage.

RISK 20 OF 25 · PRACTICAL DIGITAL RISK ROADMAP

What should you fix first?

SMEs don't need a 200-page technical report. They need prioritisation.

What you can do:
1. List your top five worries. For each: *Could this stop us trading? Could the fix be in within 30 days?*

2. For each remaining risk, write the smallest next action.

3. Put names against each action. No name = no action.

RISK 21 OF 25 · PHISHING & SOCIAL ENGINEERING

Can your staff spot a phishing email when it matters?

Phishing is the most common way attackers get into SMEs.

What you can do:
1. Add the Microsoft 365 or Google **Report Phishing** button to staff inboxes.

2. Forward suspicious emails to report@phishing.gov.uk.

3. Run one phishing simulation a quarter. Use it to train, not blame.

RISK 22 OF 25 · MOBILE AND REMOTE WORK SECURITY

Are phones, tablets and home laptops your weakest link?

Most SME data leaves the office every day on phones and laptops.

What you can do:
1. Enable **Mobile Device Management** for any device that accesses work data.

2. Require passcode and biometric on every device. Require encryption.

3. Test the **remote-wipe** flow once a year.

RISK 23 OF 25 · MALWARE AND ENDPOINT PROTECTION

Is your antivirus actually protecting you?

Legacy antivirus catches known viruses by signature. Modern threats bypass that.

What you can do:
1. If you have M365 Business Premium, you already have **Defender for Business**. Cancel duplicate antivirus.

2. Make sure protection is on **every** device, including home / BYOD.

3. Either have your IT supplier read the alerts, or set them to email a named person.

RISK 24 OF 25 · PATCHING & VULNERABILITY MANAGEMENT

Are you running months-old, patched-everywhere-else software?

Most ransomware uses vulnerabilities patched months earlier. Patching is the most effective single security activity.

What you can do:
1. Set **Windows Update** / **macOS Update** to automatic on all laptops.

2. For servers and network kit, agree a patching cadence with your IT supplier in writing.

3. List software past End-of-Life (Windows 7, Server 2012 R2 / 2016 in many cases). Replace, segment, or accept the risk with a date.

RISK 25 OF 25 · STAFF TRAINING & SECURITY CULTURE

Does your team know what to do when something feels wrong?

A trained, alert team is a better defence than most tools.

What you can do:
1. Roll out the free NCSC Top Tips for Staff.

2. Run one tabletop exercise a year using NCSC Exercise in a Box.

3. Make reporting easy and praise the people who do it — even on false alarms.