SME Digital Advisor

Plain-English advice on digital risk

SCENARIOS · 10 CARDS

Scenarios Flashcards

Step-by-step playbooks summarised for quick reference.

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

Companion to andrewreaassociates.com

smedigitaladvisor.co.uk

SCENARIO · INCIDENT RESPONSE

An employee just clicked a phishing email

Speed matters. The actions you take in the first hour decide whether this becomes a footnote or an incident.

First 5 minutes — contain
• **Isolate the device:** disconnect from network. Don't power it off — that destroys memory evidence.
• Tell the employee they did the right thing reporting it. Blame kills future reporting.

First 15 minutes — lock the account
• **Reset the password** from a different device.
• **Revoke active sessions** in Microsoft 365 or Google.
• Confirm **MFA** is enabled. If not, enable it now.

First 30 minutes — find the damage
• Check the mailbox for **inbox rules** the attacker may have added.
• Check the **Sent Items** for outbound phishing.
• Look at **sign-in logs** for unusual locations.

SCENARIO · INCIDENT RESPONSE

Ransomware just hit. First 24 hours

Don't pay yet. Don't reboot. Don't restore over a still-infected system.

First 30 minutes — contain
• **Isolate the affected systems** from the network. *Do not power off.*
• Disconnect **shared drives and backup targets**.
• Tell staff: **stop using IT**.

First hour — call
• **Your IT supplier.**
• **Your cyber insurer.** Most policies require notification within hours.
• **The incident-response retainer**, if you have one.

First few hours — document
• **Photograph the ransom note** and encrypted file extensions.
• Record **who noticed what, when**.
• Identify the **scope**.

SCENARIO · PEOPLE

A staff member is leaving. Managing their access

Leavers are the most common source of orphaned accounts.

One week before
• List every system they have access to.
• Identify what they own (files, dashboards, automations). Brief their manager.
• Identify external accounts in their personal email.

Day of departure
• **Disable** the M365 / Google account at end of day — don't delete.
• **Revoke MFA enrollment**.
• **Sign out of all sessions**.

Within a week
• Audit **shared drives**. Reassign ownership.
• Audit **external SaaS**.
• Email **external suppliers** to update contacts.

SCENARIO · PEOPLE

IT onboarding for a new joiner

A consistent process prevents 80% of access problems three years later.

Pre-day-1
• Decide their **role** and grant access by role.
• Create the account, but **don't enable** until day 1.
• Provision encrypted, MFA-enrolled, EDR-protected hardware.

Day 1
• Help them **enrol MFA** — authenticator app, not SMS.
• Set them up in the **password manager**.
• Walk through the **AI usage policy** and acceptable use.

First week
• Schedule a **15-minute social engineering brief**.
• Confirm they have ONLY what they need.
• Add them to the **tools register**.

SCENARIO · CUSTOMERS

A customer just sent us a security questionnaire

These are now routine. The first one is hard; the tenth is a copy-paste.

Before you answer
• Read the whole questionnaire first.
• Find out who at the customer is asking.
• Check if they'll accept a **Cyber Essentials** certificate.

Building your security pack
• A short **data-handling statement**.
• Your **policies**: data protection, password, acceptable use, incident response, AI usage.
• Evidence: MFA screenshot, backup screenshot, training records.

Answering
• **Be honest.** Lying voids your insurance.
• **If the answer is 'no', add 'here's our plan and date.'**
• Attach evidence without being asked.

SCENARIO · BUYING DECISIONS

Choosing a new IT supplier (MSP)

This decision affects your security posture more than any tool.

Decide what you actually want
• Is this **helpdesk support** only, or security, backup, patching?
• How many users / devices? Hours of cover?
• What is “in scope” vs “projects extra”?

Ten questions to ask
• Are you Cyber Essentials Plus certified?
• What do you do for our security beyond support tickets?
• How do you test backups? Show me a recent report.

Red flags
• Vague answers about security.
• Refusal to do test restores.
• Default policy of owning the domain or master admin.

SCENARIO · BUYING DECISIONS

Choosing cyber insurance

Cyber insurance has matured. The cover is more useful and the requirements stricter.

Do you need it?
• What would a 5-day outage cost you?
• What would notifying customers cost?
• Do any of your customer contracts *require* cyber insurance?

What good cover usually includes
• Incident response: technical, forensic, legal, PR.
• Business interruption.
• Data restoration costs.

Common gaps to ask about
• **Social engineering / BEC fraud.**
• **Ransom payments.**
• **Supplier failure.**

SCENARIO · STANDARDS

Approaching Cyber Essentials

Achievable in 4–8 weeks for most SMEs.

The five controls
• **Firewalls.** Every device has a properly-configured firewall.
• **Secure configuration.** Default passwords removed.
• **User access control.** Admin rights rare and reviewed; documented leaver process.

Typical 4-week run
• **Week 1.** Download IASME questionnaire. Identify gaps.
• **Week 2.** Fix easy ones (MFA, remove local admin).
• **Week 3.** Harder ones (patching schedule, EDR, leaver process).

Cyber Essentials vs Cyber Essentials Plus
• **CE**: self-assessed.
• **CE Plus**: external technical check. Often required for government contracts.

SCENARIO · AI

Adopting AI safely in a small team

You don't need a moratorium. You need a four-step plan and a one-page policy.

Step 1 — discover
• Email all staff: *"Which AI tools? What data?"*
• Cross-check Microsoft 365 admin reports.
• Look at browser history (with permission).

Step 2 — classify
• **Green:** public info. Most tools fine.
• **Amber:** internal-not-sensitive. Paid tier with training disabled.
• **Red:** customer/financial. Only tools with a clear DPA.

Step 3 — standardise
• Pick one tool the company will pay for and train on.
• Disable training-on-prompts.
• Train staff on the chosen tool.

SCENARIO · M&A

Buying or being bought — the IT bit

The hidden costs in a deal are usually in IT and data.

Documents to request
• Asset list: hardware, software, SaaS, domains.
• Supplier list with contract end dates.
• Policies and incident history.

Red flags
• No incident response plan.
• No tested backups.
• Single IT contractor with no handover.

Questions for the IT supplier and CTO
• What three risks are you actively managing?
• Worst incident in 3 years?
• Who owns the domain, DNS, master admin?