

SME Cyber Acronym Quick Cards

Short plain-English cards for the terms most likely to matter in small business conversations.

VERSION 1.0 | REVIEWED 5 AUGUST 2026 | COPYRIGHT (C) 2026 ALDERMERE SYSTEMS. ALL RIGHTS RESERVED.

DO I NEED
TO CARE?

Yes. This is one of the most important basic protections a business can use.

MFA / 2FA

Multi-Factor Authentication / Two-Factor Authentication

MFA means logging in with more than just a password. For example, you enter your password and then approve the login using an app, code, fingerprint or security key.

Why it matters

Passwords get stolen, guessed and reused. MFA helps stop criminals getting into accounts even if they know the password.

SME action

Turn MFA on for email, banking, Microsoft 365, Google Workspace, accounting software, website admin accounts, cloud storage and anything holding customer or payment information.

DO I
NEED TO
CARE?

Yes, especially if customers, insurers or public sector buyers ask about your cybersecurity.

CE / Cyber Essentials

Cyber Essentials

Cyber Essentials is a UK cybersecurity certification that checks whether your business has basic protections in place.

Why it matters

It helps show that your business takes cybersecurity seriously. It may also be requested when bidding for certain contracts or working in supply chains.

SME action

Check whether your business could pass the basic Cyber Essentials requirements. Focus on secure settings, updates, access control, malware protection and firewall protection.

DO I NEED TO
CARE?

Maybe. It depends who you
sell to.

CE+ / Cyber Essentials Plus

Cyber Essentials Plus

Cyber Essentials Plus is the stronger version of Cyber Essentials because it includes independent technical testing.

Why it matters

Some customers may trust Cyber Essentials Plus more because it is not just a self-assessment.

SME action

Start with Cyber Essentials first. Consider Cyber Essentials Plus if you work with larger clients, public sector buyers, sensitive data or regulated industries.

DO I NEED TO
CARE?

Yes, if your business handles
personal data.

GDPR / UK GDPR

General Data Protection Regulation / United Kingdom GDPR

UK GDPR is the law covering how organisations collect, store, use, share and protect personal information.

Why it matters

Customer names, email addresses, phone numbers, addresses, employee records, order histories and marketing lists can all count as personal data.

SME action

Know what personal data you hold, why you hold it, where it is stored, who can access it and how long you keep it.

DO I NEED TO
CARE?

Yes, if your business handles
personal data.

ICO

Information Commissioner's Office

The ICO is the UK regulator for data protection and information rights.

Why it matters

The ICO provides guidance for businesses and can deal with complaints or data protection issues.

SME action

Use ICO guidance when writing privacy notices, handling customer data, managing cookies or dealing with data requests.

DO I NEED TO CARE?

Sometimes.

DPIA

Data Protection Impact Assessment

A DPIA is a risk assessment for privacy. It helps you think through whether a project could create risks for people's personal data.

Why it matters

A DPIA may be needed when using sensitive data, monitoring people, introducing new technology or doing something that could affect privacy.

SME action

Carry out a DPIA before launching systems that involve sensitive personal data, tracking, surveillance, profiling or unusual use of customer information.

DO I NEED
TO CARE?

Yes, if you store personal data about customers, staff or users.

SAR / DSAR

Subject Access Request / Data Subject Access Request

A SAR is when someone asks to see what personal data your business holds about them.

Why it matters

Businesses need to know how to recognise and respond to these requests properly.

SME action

Have a simple internal process for handling personal data requests. Make sure staff know who to pass them to.

DO I NEED
TO CARE?

Yes, if you rely on email for customers, invoices, bookings or marketing.

DKIM

DomainKeys Identified Mail

DKIM adds a digital signature to outgoing email so receiving systems can check that the message has not been tampered with.

Why it matters

It helps prove that your email is legitimate.

SME action

Make sure DKIM is enabled in Microsoft 365, Google Workspace, Mailchimp, Shopify or whatever platform sends email on your behalf.

DO I NEED
TO CARE?

Yes, if your business sends email from its own domain.

SPF

Sender Policy Framework

SPF is a domain setting that says which mail servers are allowed to send email for your business.

Why it matters

It helps reduce fake emails pretending to come from your domain.

SME action

Ask your domain, website or IT provider whether SPF is correctly set up for your business email.

DO I NEED
TO CARE?

Yes. This is becoming increasingly important for business email trust.

DMARC

Domain-based Message Authentication, Reporting and Conformance

DMARC tells receiving mail systems what to do when an email fails SPF or DKIM checks.

Why it matters

It helps stop criminals spoofing your domain and pretending to be your business.

SME action

Set up DMARC carefully. Start with monitoring, then move towards stricter protection once legitimate email sources are confirmed.

DO I NEED
TO CARE?

**Yes, especially if your business has
laptops, desktops or servers.**

EDR

Endpoint Detection and Response

EDR watches devices for suspicious activity and helps detect attacks that basic antivirus may miss.

Why it matters

Modern attacks do not always look like traditional viruses. EDR can spot unusual behaviour, such as strange scripts, stolen credentials or attacker movement.

SME action

Ask your IT provider what protection is installed on business devices. Do not assume basic antivirus is enough for every situation.

DO I NEED TO
CARE?

**Yes, but do not treat it as a
magic shield.**

VPN

Virtual Private Network

A VPN creates a secure connection between a device and another network or service.

Why it matters

VPNs are often used for remote access to business systems. Poorly configured VPNs can also become a target.

SME action

Use VPNs only where needed, keep them updated, protect them with MFA and remove access for people who no longer need it.

DO I NEED
TO CARE?

**Yes. Every business should have at
least a simple version.**

BCP

Business Continuity Plan

A BCP explains how the business keeps going during disruption.

Why it matters

Cyberattacks, power cuts, internet outages, supplier failures and lost devices can all stop work.

SME action

Write down what happens if email, payments, website, phones, files or key software are unavailable.

DO I NEED TO CARE?

Yes.

DR

Disaster Recovery

Disaster recovery is how you restore systems, files and data after a serious failure.

Why it matters

Backups are only useful if they can actually be restored.

SME action

Check that backups exist, are recent, are protected from ransomware and have been tested.

DO I NEED TO CARE?

Yes, if downtime costs your business money.

RTO

Recovery Time Objective

RTO means how quickly you need a system back after it fails.

Why it matters

Some systems can be down for a day. Others need to be restored within an hour.

SME action

Decide which systems are critical and how long the business can survive without each one.

DO I NEED TO CARE?

Yes, if losing data would hurt the business.

RPO

Recovery Point Objective

RPO means how much data you can afford to lose.

Why it matters

If your backup runs once per day, you may lose up to a day's work.

SME action

For critical systems, make sure backup frequency matches the amount of data loss the business can tolerate.

DO I NEED TO CARE?

Yes, if you outsource IT.

MSP

Managed Service Provider

An MSP is an external company that manages IT support, devices, updates, users, networks and systems.

Why it matters

Many SMEs rely on MSPs, but not all MSPs provide the same level of security.

SME action

Ask exactly what is included: updates, backups, MFA, device protection, monitoring, documentation and incident support.

DO I NEED TO CARE?

Maybe.

MSSP

Managed Security Service Provider

An MSSP is a provider focused specifically on cybersecurity services.

Why it matters

An MSP may handle general IT, while an MSSP may provide monitoring, response, vulnerability management and security advice.

SME action

Consider MSSP support if your business handles sensitive data, has compliance obligations or cannot monitor security internally.

DO I
NEED TO
CARE?

Yes, if your business uses AI tools, integrations, payment systems or connected software.

API Key

Application Programming Interface Key

An API key is a secret code that lets one piece of software access another service.

Why it matters

If an API key is leaked, someone else may be able to use your account, access data or create charges.

SME action

Treat API keys like passwords. Do not paste them into public websites, screenshots, documents or support chats.

DO I NEED TO
CARE?

Yes, if using AI or cloud-connected tools.

BYOK

Bring Your Own Key

BYOK means the user supplies their own API key instead of the software provider holding or reselling access.

Why it matters

It can give the customer more control, but it also means the customer must manage the key safely.

SME action

Use separate keys for separate tools where possible. Revoke keys that are no longer needed.

DO I NEED
TO CARE?

Yes, especially for reputation, security and fraud prevention.

OSINT

Open Source Intelligence

OSINT means information gathered from public sources such as websites, company records, search engines, social media and public documents.

Why it matters

Attackers, scammers and competitors can use public information about your business. You should know what is visible.

SME action

Search for your business, directors, email addresses, old documents, exposed files and outdated public information.

DO I
NEED TO
CARE?

Maybe. Most small businesses do not need to run one themselves, but they should understand the term.

SIEM

Security Information and Event Management

A SIEM collects logs from systems and helps identify suspicious activity.

Why it matters

It can help detect attacks, but it needs proper setup and monitoring.

SME action

If a provider mentions SIEM, ask who monitors it, what alerts are reviewed and what happens when something serious is found.

DO I NEED TO
CARE?

Maybe, depending on business
size and risk.

SOC

Security Operations Centre

A SOC is a team that monitors security alerts and responds to cyber incidents.

Why it matters

Security tools are only useful if someone pays attention to the alerts.

SME action

Ask whether your provider offers real monitoring or simply installs tools and leaves them running.

DO I
NEED TO
CARE?

Usually only if your business works in
regulated, essential or important
services.

NIS

Network and Information Systems

NIS rules focus on the cyber resilience of important services and digital infrastructure.

Why it matters

Some organisations have specific legal duties because the services they provide are important to society or the economy.

SME action

If you supply public sector, healthcare, energy, transport, digital infrastructure or other critical sectors, check whether your customers expect NIS-related controls from suppliers.

DO I
NEED TO
CARE?

Potentially, especially if your business
supplies regulated sectors or critical
services.

CSR Bill

Cyber Security and Resilience Bill

This is UK legislation intended to update cyber resilience rules and strengthen protection for important services.

Why it matters

Even where SMEs are not directly regulated, larger customers may pass cyber requirements down through contracts and supplier checks.

SME action

Watch for supplier security requirements from customers in healthcare, public sector, digital services and critical infrastructure.

