Cyber Security

Build a security-first culture **across your organisation**

www.breathetechnology.com

breathetechnology

support | cloud | security | infrastructure | comms

Empowering You Through Secure Technology

*It's rare that you think about **cyber security** until something interrupts your working day.*

A strange email gets opened or somebody suddenly can't access their account. Files disappear. Perhaps a supplier calls asking why they've received a payment request.

It's then you stop and realise how much modern systems depend on trust.

Trust that the right people can access the right information. That staff will spot something suspicious before it becomes a problem. And that the systems holding your customer, pupil, staff or business data are properly protected.

Most organisations already have some security in place. There's usually antivirus software, backups, passwords, maybe a firewall.

The challenge is that modern security risks aren't always obvious.

Many start during completely normal moments.

Someone is rushing between meetings, lessons or appointments and logs into what looks like Microsoft 365.

An employee shares access to something because a colleague needs it urgently.

A staff member leaves and their accounts remain active because removing them drops down the priority list.

A teacher, employee or senior leader clicks a link they weren't expecting, simply because it looks legitimate.

It's everyday working life. And that's what makes security difficult.

It's also why organisations that are managing modern security risks well are looking beyond technology. They're building a culture where security becomes part of how people work, whether that's in a school, academy trust, charity or business.

When good habits become part of how people work, security improves almost naturally.

What a security-first culture **looks like**

When people hear the phrase **"security-first culture",** they often imagine strict rules and nervous employees afraid to touch anything.

But the healthiest organisations usually feel relaxed. People aren't frightened of technology. They understand how to use it safely and know what to do when something doesn't look right.

You can normally tell within a few conversations how an organisation approaches security.

In some businesses and schools, staff share passwords casually because it feels quicker.

Access to files grows over the years until almost everybody can see almost everything. Nobody is completely sure who still has access to old systems. Nothing bad has happened yet, so the issue never reaches the top of the list.

Other organisations feel different.

Employees check unusual requests before acting on them. Access to systems is reviewed and managed properly. When someone leaves, there's a clear process for removing their access rather than a vague mental note to "sort it later".

It becomes part of how the organisation operates.

Security works best when it stops feeling like a separate technical issue sitting in the corner and becomes part of normal decision making.

The organisations that handle this well usually haven't achieved it through fear or endless policy documents, which most people don't read properly anyway.

They've built it through repetition, communication, and sensible routines that people understand.

Why organisations fall **into bad habits**

Businesses and schools are busy places.

People multitask constantly. Managers, gteachers and support staff often wear several hats. Somebody in finance is helping with operations while answering emails about recruitment and trying to chase an overdue invoice at the same time.

In that environment, convenience wins. Everybody is trying to keep things moving.

But that's how bad habits develop.

Passwords get reused because there are already too many to remember.

Access gets shared because somebody needs something urgently.

Software updates get postponed because nobody wants systems restarting during the working day.

Most of these decisions feel harmless. They're practical decisions made by busy people.

Over time, however, an organisation can collect years' worth of small shortcuts that nobody has properly reviewed.

One of the biggest misconceptions about cyber security is that organisations become vulnerable because their people are careless.

Usually, the reality is much more ordinary. People are simply working quickly, often under pressure, within systems and processes that may not have been reviewed for some time.

And unfortunately, modern cyber criminals understand exactly how organisations operate.

They know people are busy. They know someone will eventually click a convincing email while trying to clear a crowded inbox. And they know that creating a sense of urgency can influence even experienced people.

That's why phishing emails have become so convincing.

A phishing email is a fake message designed to trick someone into clicking a link, opening a file or entering their login details.

Years ago, these emails were often easy to spot because they looked suspicious immediately.

Today, they can look almost identical to genuine messages from suppliers, delivery companies, banks, Microsoft, or even people you work with every day.

Why leadership **is important**

One thing becomes obvious when you work with organisations for long enough: People pay close attention to leadership behaviour.

If managers ignore security processes whenever they become inconvenient, staff notice.

If a business leader, school leader or senior member of staff regularly asks someone to share a password "just this once", that quickly becomes accepted behaviour.

The opposite is true as well.

When leadership follows the same processes as everyone else, people take them more seriously.

And thankfully, good leadership around security doesn't require technical expertise.

You don't need to understand firewalls or encryption in detail. What matters more is the attitude around decision-making.

- Do people feel comfortable reporting concerns?
- Do managers encourage sensible checking rather than rushing?
- Are systems and access reviewed properly when staff join or leave?
- Do people understand what is expected of them?

These things shape security culture far more than annual training sessions alone.

An organisation can invest heavily in security technology and still face avoidable risks because basic internal habits have never improved.

Equally, an organisation with simpler systems can operate securely when the culture around technology is healthy.

People check things. Questions are encouraged. Processes are clear.

Consistency makes a huge difference.

Making secure behaviour **simpler**

One of the smartest things an organisation can do is reduce the amount of effort required to work securely.

If something feels awkward or frustrating, people will naturally look for workarounds.

Take passwords as an example.

Most people now have dozens of accounts across different systems. Expecting employees to remember unique, complex passwords for every single one without any support is unrealistic.

That's where **password managers** help.

A **password manage**r securely stores passwords for staff, which means they only need to remember one strong password instead of fifty different ones.

It usually improves security immediately because people stop relying on familiar favourites they've been reusing since around 2014.

Multi-factor authentication helps in a similar way.

That's the extra step where you confirm a login using your phone or an authentication app after entering your password. It adds a few seconds to the login process, but it prevents a huge number of account compromise attempts.

Good security often comes down to building systems that support people properly instead of expecting perfect behaviour all the time.

The same applies to reporting problems.

If staff aren't sure who to contact about a suspicious email, many simply ignore it and carry on.

If there's a simple reporting process and a culture where questions are welcomed, problems get spotted much earlier.

You want staff to feel comfortable enough to pause and check when something feels unusual.

Short conversations **work better than annual training**

Most people have experienced terrible security training at some point.

A long presentation, endless slides, statistics nobody remembers. By the end, half the room is mentally planning dinner.

The organisations getting the best results usually handle awareness differently.

Security becomes part of normal conversation.

- A quick reminder about a new phishing scam that's doing the rounds.
- A short discussion during a team meeting.
- A real example of how a business nearby was caught out.

Those smaller conversations tend to stick because they feel relevant to everyday work.

And importantly, people need to feel safe admitting mistakes.

If somebody clicks something suspicious, the priority should be resolving the problem quickly, not embarrassing them in front of the team.

Organisations where staff are afraid to admit mistakes often discover problems much later than they should.

That delay can turn a manageable situation into a much larger one.

The strongest security cultures have plenty of small checking conversations happening every week.

"Does this email look right to you?"

"Were you expecting this file?"

"Can you just double-check this payment request before I send it?"

Putting the right protection **around the organisation**

Good habits are incredibly important, but they still need supporting with sensible technical protection.

That includes things like keeping software updated, protecting devices properly, filtering suspicious emails, reviewing who has access to systems, and making sure backups are working.

Backups are particularly important because they give you a way to recover information if something goes wrong.

They do need testing occasionally.

A backup that has never been checked properly can create an unpleasant surprise when you need it.

It also helps to think carefully about access.

Most people don't need access to everything within an organisation.

Modern systems allow access to be based around somebody's role, which keeps things much easier to manage.

If an account is compromised, the damage is limited when permissions are controlled properly.

This becomes especially important as organisations grow, because systems naturally become more complicated over time. More staff, software, suppliers, and more devices connecting remotely.

Without regular reviews, it becomes increasingly difficult to keep track of who can access what.

Building something stronger **over time**

Most organisations strengthen security gradually, through a series of sensible improvements:

- **Clearer processes around staff access**
- **Better password protection**
- **More awareness across the team**
- **Regular reviews of systems and permissions**
- **Better conversations internally**

The organisations that handle this best usually are the ones where sensible habits have become part of normal working life.

That creates confidence.

People know what to do if something feels wrong. Leadership understands where the biggest risks sit, and systems are reviewed before problems appear, instead of afterwards.

All it needs is attention and consistency.

Most organisations are already much closer to this than they think. They usually just need somebody to help connect the dots, tighten a few processes, and make sure the foundations underneath everything are solid.

That's where a good IT support partner can make a real difference, by helping you build an organisation where security supports the way your team already works.

If you're ready to build a stronger, more security-aware organisation without making day-to-day work harder for your team, we'd love to help.

Get in touch.


www.breathetechnology.com
(live chat available)


London 020 3519 0124
Cambridge 01223 209920
Sheffield 0114 349 8054
Suffolk 0144 059 2163


lucy@breathetechnology.com

breathetechnology
support | cloud | security | infrastructure | comms

Empowering You Through Secure Technology