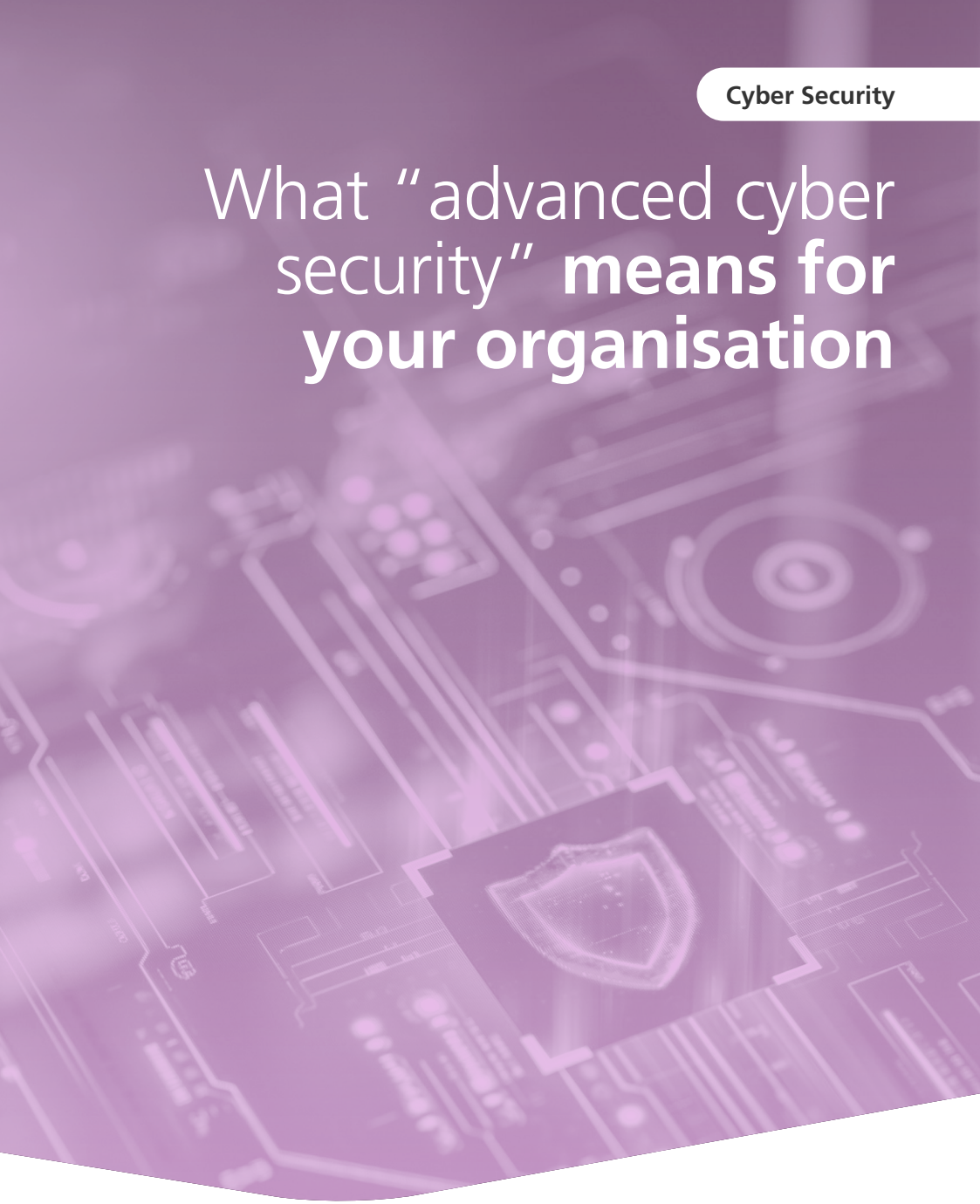
Cyber Security

What "advanced cyber security" **means for your organisation**



www.breathetechnology.com

breathetechnology

support | cloud | security | infrastructure | comms

Empowering You Through Secure Technology

When was the last time you set aside time to review your cyber security?

For most organisations, it isn't something that's planned. It usually comes up another way.

A customer, parent, client or stakeholder asks how their data is protected.

A regulator, auditor or governing body wants more information.

Or you hear about another organisation having a cyber security incident and it makes you stop and think.

That's when a few simple questions start to come up.

- **Who can access our systems?**
- **Where is our data actually stored?**
- **How well is it protected?**

And for many organisations, the honest answer is… "It's not completely clear."

New systems get added, people are given access so they can get on with their work, and technology evolves over time without anyone stepping back to review the bigger picture.

It's how things happen as organisations grow.

When you handle sensitive information, the risks become greater.

Whether you are protecting customer, financial data or employee data, or pupil and safeguarding record, there are increasing expectations around how that data is managed and protected.

Organisations with regulatory, legal or safeguarding responsibilities need to understand where their data is, control who can access it, and be able to demonstrate that appropriate security measures are in place.

Cyber security has evolved to reflect this.

It's no longer just about ticking boxes. It's about understanding how your organisation operates, who has access to what, where risks exist and how prepared you are if something goes wrong.

When people hear "advanced cyber security", it can sound complicated or overwhelming.

In reality, it's about getting the important things right – improving visibility, strengthening protection and making sure your organisation is better prepared when challenges arise.

For many organisations, the systems and security tools are already there. They have been added over time, but they are not always joined up in a way that makes security easy to understand, manage and improve.

The risks have changed (and so have the consequences)

Cyber threats aren't what they used to be.

They are more focused, more deliberate and increasingly aimed at organisations that hold valuable information – including personal, financial, employee, customer, pupil or safeguarding data.

One of the most common ways attackers get in is through something called phishing. This is where an email is designed to look genuine and encourages someone to click a link, open an attachment or enter their login details.

And these emails can be very convincing.

They might appear to come from a supplier, a colleague or a service you already use. When you're busy, it's easy to take them at face value.

For example, someone in your organisation receives an email that appears to come from a supplier. It asks them to log in to view an updated document. The link looks genuine, so they enter their details and carry on.

Nothing happens straight away.

Later, that account is used to access emails, reset passwords or request payments.

From the outside, everything can look like normal activity, making it harder to spot early.

Ransomware is another common issue. This is when attackers gain access to your systems and prevent you from accessing your data. They then demand payment to restore access.

In some cases, they also take a copy of the data before disrupting your systems. This creates another concern, as you need to understand what information may have been accessed and where it could end up.

There are also situations where data is accessed without permission. For organisations with legal, regulatory or safeguarding responsibilities, this can create further challenges.

You may need to report what has happened, investigate the impact and explain how it is being managed.

The impact goes beyond technical.

It affects how your organisation operates, how people trust you and how much time your teams spend responding.

Investigating what happened, answering questions and putting things right can quickly take focus away from your core activities.

You might:

- *Lose access to key systems*
- *Experience disruption to day-to-day operations*
- *Need to inform customers, parents, partners or other stakeholders*
- *Face questions from regulators, auditors or governing bodies*

What makes this harder is how normal things can look at the start. A login appears genuine. Activity doesn't immediately stand out. Nothing feels obviously wrong.

That's why modern security needs to focus on behaviour as well as protection – understanding what normal activity looks like, identifying unusual behaviour and responding quickly when something changes.

Why basic IT security is **no longer enough**

Most organisations already have some level of protection in place.

You may have security software that helps detect harmful programmes. You may have a firewall that helps control how your systems connect to the outside world.

These are still important and should always be part of your security approach.

The challenge is that many modern attacks no longer try to force their way in. They log in instead.

If someone has a valid username and password, systems can often treat them as a genuine user. From the system's point of view, the activity may look completely normal.

There are also everyday habits that can gradually increase risk.

- Access is given more widely because it is ***quicker.***
- Passwords are reused because it is ***easier.***
- Accounts remain active because removing them ***is not seen as urgent.***

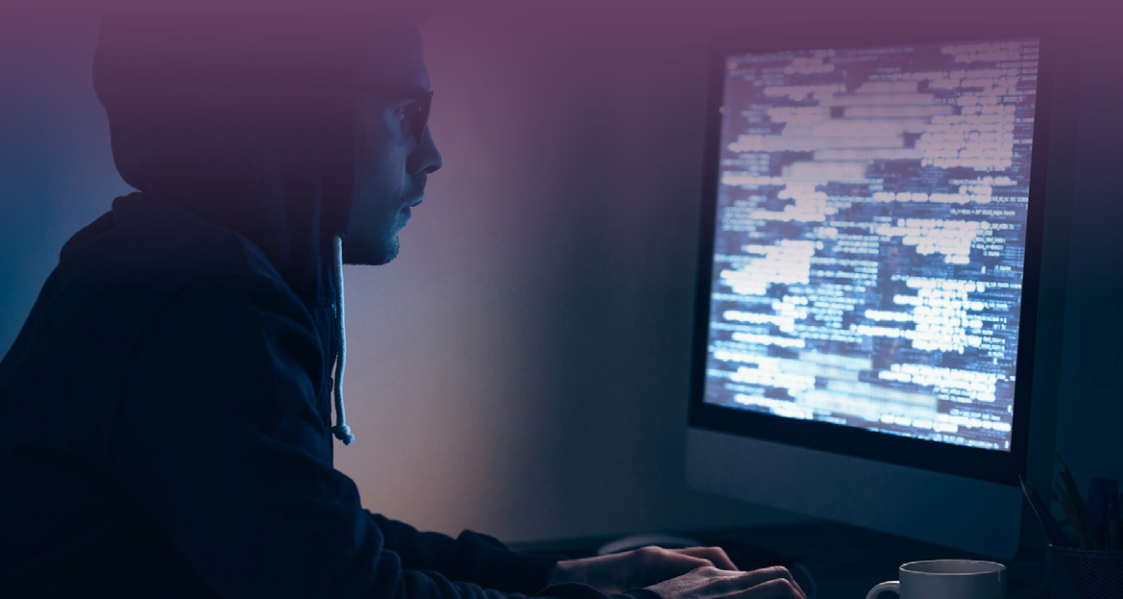
This is how organisations operate when people need to get work done. But over time, it can create an environment where it becomes harder to understand who has access, what they can see and what they are able to do.

Security now needs to reflect the way people work. That means considering remote access, mobile devices, cloud services and the growing number of users who need access to systems.

It means understanding:

- Who can access your systems
- What information they can reach
- Whether that access is still appropriate
- How that activity is monitored and managed

Modern cyber security is about having visibility and control, not just putting barriers in place.



What advanced cyber security **looks like**

When you break it down, advanced cyber security is not about adding lots of complicated tools.

It is about getting the right foundations in place and making sure the different areas of security work together.

When these areas are properly connected and managed, they give you greater visibility, help reduce risk and provide a clearer picture of what is happening across your organisation.

Controlling access

Access is at the centre of most security issues.

It helps to start with a simple question: what does each person actually need to access to do their role?

When access is based on responsibilities, it becomes easier to manage and reduces risk if an account is compromised.

Multi-factor authentication adds another layer of protection.

You have probably experienced this when logging in and being asked for a code from your phone or an authentication app.

That extra step makes it much harder for someone else to gain access, even if they have obtained a password.

Protecting devices

Every device that connects to your systems plays a part in your overall security.

This includes laptops, mobile devices, desktops and other connected equipment.

These devices need to be kept up to date and configured correctly so that organisational data remains protected.

If a device is lost, stolen or compromised, you need to be able to respond quickly by removing access, securing the device or protecting the data stored on it.

Securing data

Your data is one of your organisation's most important assets.

Protecting it means controlling who can access it, keeping it secure and ensuring you can recover it if something goes wrong.

Encryption helps protect information by making it unreadable without the correct access.

Backups provide a way to restore data after an incident. But it is equally important to understand how your backups work, whether they are protected and how quickly you could recover when you need them.

Monitoring activity

Monitoring gives you visibility of what is happening across your systems.

If something unusual happens, such as a login from an unexpected location or access to information that does not match someone's role, it can be identified and investigated.

This helps you respond earlier, before a small issue becomes a bigger problem.

It also gives you more confidence day to day, because you are not relying on security problems becoming obvious before you notice them.

The human factor **(why people remain a key part of security)**

People are a big part of how systems work, and attackers know this.

Many cyber attacks are designed around human behaviour rather than technology alone. Phishing emails are a common example.

They are designed to look familiar and create a sense of urgency. It might be a message that appears to come from a colleague asking for something quickly, or from a supplier requesting an update.

When people are busy, it is easy to respond without thinking too much about it.
There are also smaller, everyday actions that can increase risk:

- Passwords may be reused across systems
- Files may be shared more widely than intended
- Access may not be removed quickly enough when someone leaves

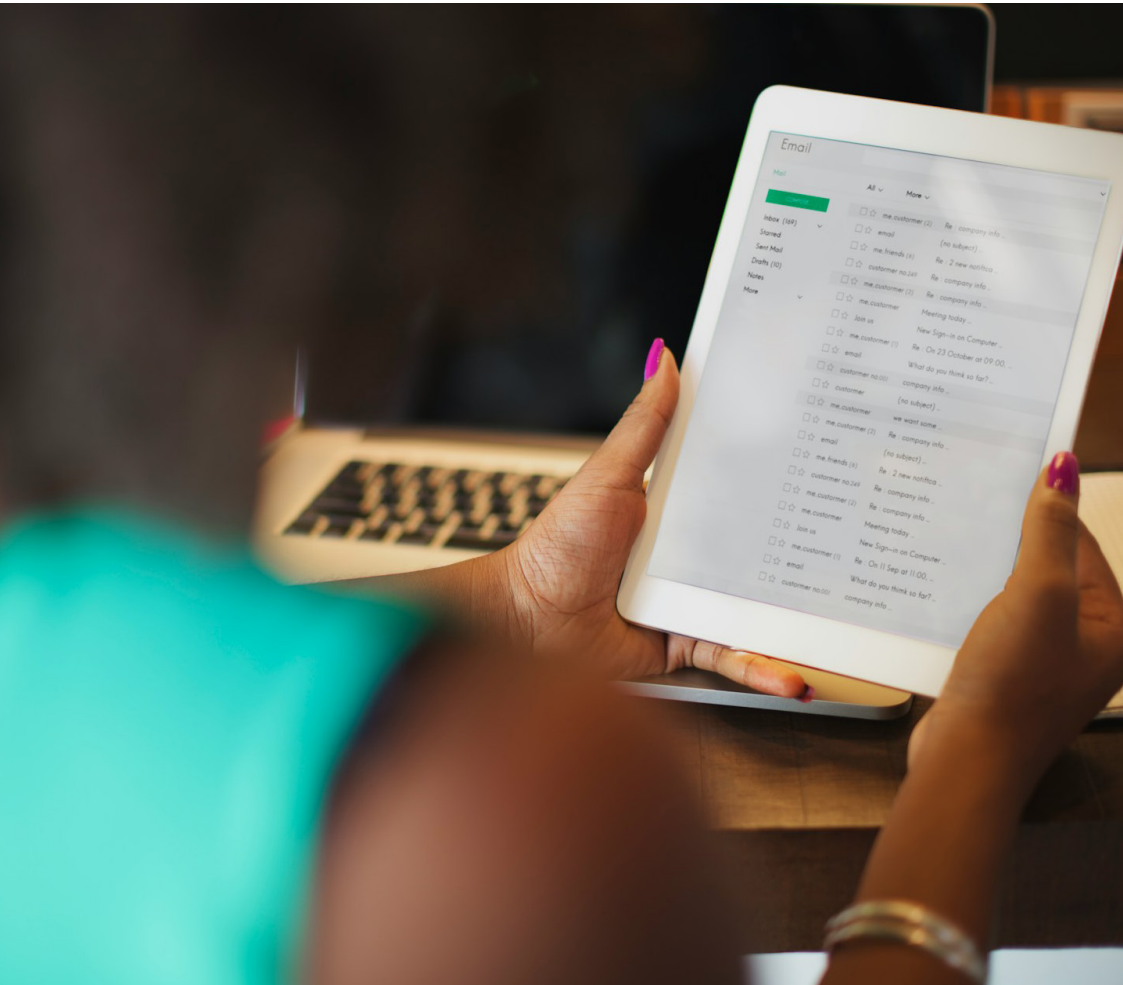
These things can happen as part of normal day-to-day work.

The aim is not to make people nervous or overly cautious. It is to help everyone recognise potential risks, understand what to look out for and feel confident raising concerns.

A little awareness can make a significant difference.

It also helps create a culture where asking questions is encouraged. If something feels unusual, people should feel comfortable checking before acting.

That short pause can prevent a situation from developing further, especially when attackers use urgency, authority or pressure to influence decisions.



Responding to a **cyber security incident**

Even with strong security in place, incidents can still happen.

The difference is often how quickly and effectively your organisation responds.

An incident response plan is simply a clear, agreed approach to dealing with a cyber security incident.

It sets out who needs to be involved, what actions to take and how information should be communicated.

If an account is compromised, that might mean securing access, investigating what has happened and assessing whether any systems or data have been affected.

Depending on your organisation and the type of incident, you may also need to report it and inform the appropriate people, regulators or authorities.

Having a plan makes these situations much easier to manage.

It provides a clear course of action when decisions need to be made quickly and helps reduce confusion at a critical time.

For example, knowing who to contact first, how to contain the incident and what needs to happen during the first hour can make a significant difference to the overall impact.

How to **take control**

Improving your cyber security does not mean changing everything at once.

It starts with understanding what you have today.

- Who has access to your systems?
- Where is your data stored?
- How is it protected?

From there, you can make improvements in a structured and manageable way.

For many organisations, the first step is simply gaining a clearer picture of what is already in place.

That might involve reviewing who has access to key systems, checking how data is stored and backed up, and understanding how accounts and devices are protected.

Once that picture is clearer, it becomes much easier to prioritise improvements and reduce risk.

Small changes can make a significant difference.

Enabling multi-factor authentication, reviewing user access, strengthening backup arrangements and removing unnecessary accounts are all good places to start.

It also helps to look at how everything works together. Cyber security is most effective when access, devices, data and monitoring support one another as part of a joined-up approach.

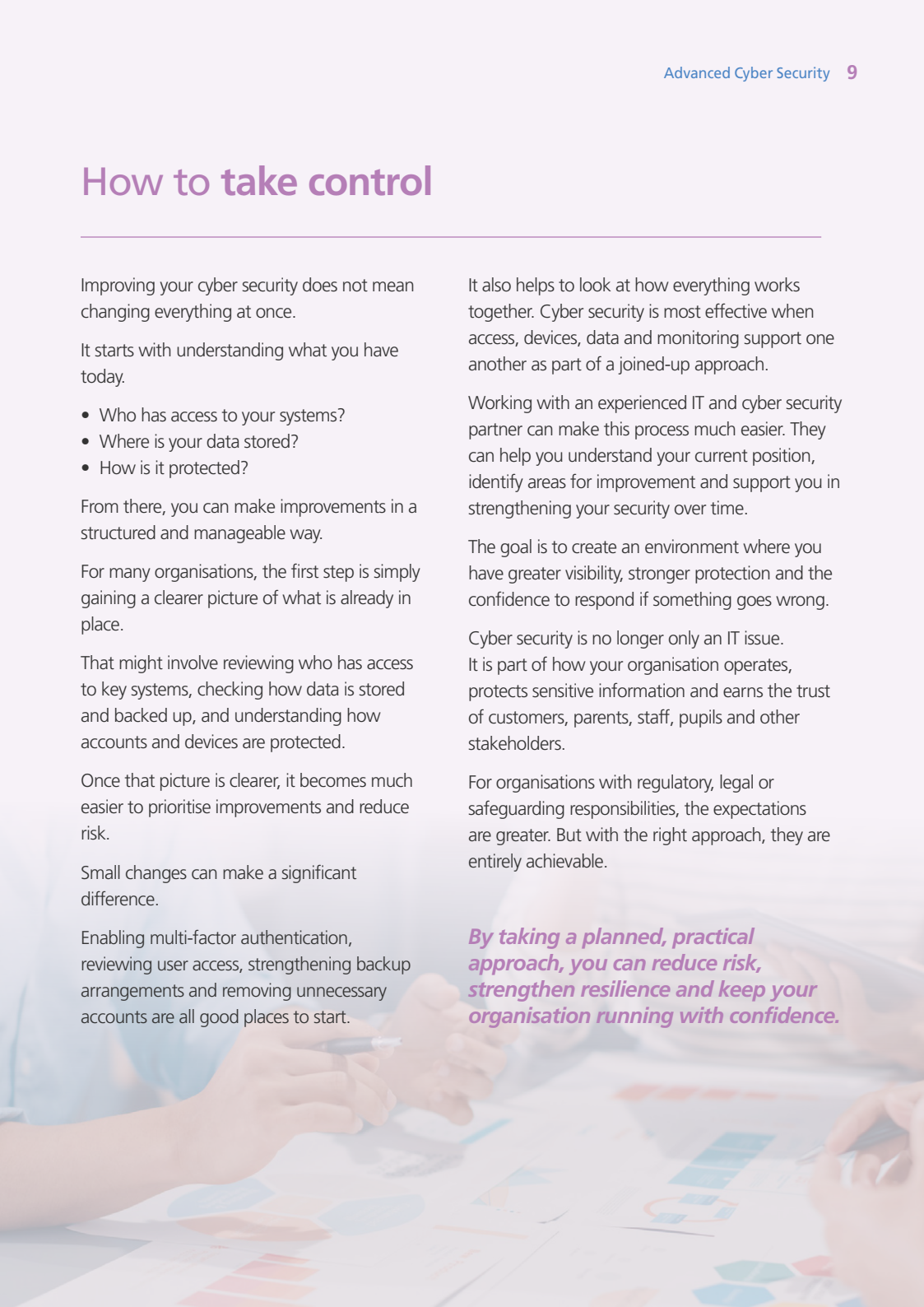
Working with an experienced IT and cyber security partner can make this process much easier. They can help you understand your current position, identify areas for improvement and support you in strengthening your security over time.

The goal is to create an environment where you have greater visibility, stronger protection and the confidence to respond if something goes wrong.

Cyber security is no longer only an IT issue. It is part of how your organisation operates, protects sensitive information and earns the trust of customers, parents, staff, pupils and other stakeholders.

For organisations with regulatory, legal or safeguarding responsibilities, the expectations are greater. But with the right approach, they are entirely achievable.

By taking a planned, practical approach, you can reduce risk, strengthen resilience and keep your organisation running with confidence.



If you'd like a clearer picture of where you stand and what to improve, we can talk it through.

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