MARCH / APRIL
2026

BITS & BYTES

CYBER ESSENTIALS

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- Lee Hewson
Founder and MD

CYBER ESSENTIALS IS CHANGING, WHY "TICK-BOX" COMPLIANCE IS NO LONGER ENOUGH

Cyber Essentials has been around for a while, and most businesses have at least heard of it.

Many have even completed it once. Job done, right?

Not anymore.

Cyber Essentials is quickly becoming a baseline requirement across multiple sectors.

Whether you are working with the public sector, part of a supply chain, or handling sensitive data, certification is often expected.

There is also a practical benefit. The scheme focuses on preventing common cyber attacks. The kind that actually hit SMEs. Phishing, weak passwords, unpatched systems.

And those attacks are not slowing down.

Why Cyber Essentials Still Matters

For many organisations, Cyber Essentials is also tied to cyber insurance.

Certification can improve your chances of getting cover and help keep premiums under control.

But the biggest shift is this. Cyber Essentials is no longer just about passing an assessment. It is about demonstrating that your security controls actually work.

That changes how businesses need to approach it.

At its core, Cyber Essentials is built on five key controls.

These have not changed, but expectations around them have.

The Five Controls

Firewalls and secure gateways remain your first line of defence.

Every internet-facing system needs protection, and default configurations should never be left in place.

Secure configuration focuses on reducing risk.

Removing unused software, disabling unnecessary accounts, and tightening system settings.

User access control is about limiting who can do what.

Not everyone needs admin rights. In fact, very few people should have them.

Malware protection is still essential. Systems need to be protected, monitored, and kept up to date.

Then there is patching. Often the most overlooked control.

Keeping systems updated remains one of the most effective ways to reduce risk.

Nothing here is complicated. But doing it consistently across a business?

That is where things start to slip.

Cyber Essentials has had a reputation. Tick the boxes, get certified, move on.

But CE is an evolving standard and some big changes are coming which mean that those thinking they can tick their way to a certificate are about to get a rude awakening.

The April 2026 updates push for real-world implementation. Not just policies on paper, but controls that actually work in practice.

Moving Beyond Tick Box Compliance

There is a stronger focus on vulnerability management. Businesses need to actively identify and fix issues, not assume everything is fine.

Remote access is another key area. With more connected machinery and remote support, secure access and MFA are now non-negotiable.

Scope has also been clarified. Cloud systems, hybrid environments, and platforms like Microsoft 365 all need proper consideration.

The bigger shift is mindset. Cyber Essentials is becoming continuous. Not annual.

This is where many SMEs struggle. Systems change, users come and go, updates get missed. Over time, compliance drifts.

Maintaining Cyber Essentials properly requires ongoing attention. That is the gap most businesses underestimate.

Getting started with Cyber Essentials can feel unclear. Most businesses are unsure where they actually stand.

That is where a Cyber Security and Compliance Assessment helps.

It provides a clear view of your current position, highlights risks, and gives a roadmap to certification.

It includes a pre-assessment, basic penetration testing, and practical recommendations you can act on quickly.

From there, the challenge is maintaining compliance.

A Practical Way Forward

This is why we developed YourSecure.

A service that treats Cyber Essentials as an ongoing process rather than a one-off exercise.

It includes certification support, continuous vulnerability management, dark web monitoring, and built-in remediation time. Regular reporting keeps everything visible.

There are three levels. Fortify, Shield, and Guardian. Each designed to match different stages of business growth and risk.

If you are serious about Cyber Essentials, start with clarity. Then build consistency.

That is what turns compliance into something that actually protects your business.

MARCH / APRIL
2026

BITS & BYTES

CHOOSING THE RIGHT IT PROVIDER JUST GOT EASIER, WHY ASSURIX MATTERS FOR SMES

Choosing an IT provider is difficult. On the surface, many look the same.

Similar services. Similar promises. Similar pricing structures.

But what happens behind the scenes can vary massively.

- How is access to your systems controlled?
- How are changes managed?
- What happens if something goes wrong at 2am?

These are not always easy questions to ask. And even harder to verify.

That is where things get risky. Because when an IT provider falls short, it is not just their problem. It becomes yours very quickly.

Assurix is designed to address exactly this issue. It gives SMEs a clearer way to understand how providers actually operate, not just what they say they do.

Assurix is a standard built specifically for IT providers, but the real benefit sits with their clients.

It gives SMEs a benchmark. A way to separate providers who have structured, well-managed processes from those who rely on best effort and good intentions.

In simple terms, it helps answer a key question.

"Can we trust this provider with our systems and data?"

It focuses on:

- How providers manage risk
- How they control access
- How they maintain security over time

Not just policies, but real delivery.

For SMEs, that level of visibility is valuable. It removes some of the guesswork and replaces it with something more concrete.

We are currently on our Assurix journey, aligning our processes with the standard and pushing for continuous improvement.

More importantly, we are involved in shaping it.

Our Head of Cyber Security and Compliance, Fern Ritchie, is part of the Assurix steering group.

That means contributing directly to how the standard develops and what "good" looks like for IT providers.

That involvement keeps us close to the detail. Not just adopting the standard, but helping refine it based on real-world experience.

For our clients, it means our approach is being measured against an emerging industry benchmark, not just internal expectations.

Quietly, but importantly, it raises the bar.

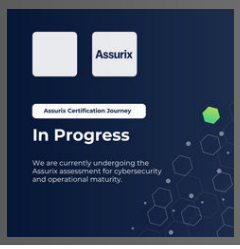
If you are working with an IT provider, or reviewing one, this matters.

Assurix gives you a way to ask better questions and expect clearer answers.

And it gives you confidence that the provider you choose is operating to a recognised standard, not just making claims.

In short, it helps you spot the difference between good and not so good.

Which is something every SME could use.



CELEBRATING SUCCESS AT THE CHAMBER AWARDS

We had a great evening at the East Midlands Chamber Nottingham Business Awards.

We were proud to sponsor the Small Business of the Year award, presented by our MD, Lee Hewson, to First Enterprise.

As Lee put it, their impact stood out. Not just their own growth, but how they have helped other local businesses and communities succeed alongside them.

We were also shortlisted for Commitment to People Development, with Leon Clarke named as a finalist for Apprentice of the Year.

We didn't take those awards home, but congratulations to the winners.

But being shortlisted still means a lot. It reflects the effort our team puts in every day, and that recognition matters.

PRACTICAL AI AGENTS FOR BUSINESS

AI agents are everywhere right now. But what do they actually do for a small business?

Our latest blog cuts through the noise and looks at practical AI agents you can start using today, without needing a data science team or a massive budget.

From automating customer responses to handling repetitive admin tasks, AI agents are quickly becoming a realistic tool for improving efficiency.

We also cover where they work best, where they don't, and what to watch out for before jumping in.

Because not every AI use case is worth your time.

If you're curious about how AI can support your business in a meaningful, low-risk way, this is a good place to start.

👉 Read the full guide:
https://www.your-itdepartment.co.uk/practical-ai-agents-for-small-business/

RANSOMWARE ATTACK ON IT PROVIDER EXPOSES CLIENTS TO SERIOUS RISK

A Managed Service Provider in Northamptonshire was reportedly hit by the Anubis ransomware group earlier this month.

According to Ransomware.live, sensitive client data has been published on the dark web, including personally identifiable information, email addresses, usernames, and passwords.

More concerning? Reports suggest this data may have been stored in plain text Word and Excel files. There are still unanswered questions, including whether all affected customers have been informed. But the wider issue is clear.

When your IT provider is compromised, your business is exposed too.

Cyber security is not just about your own systems. It extends to every supplier you trust with access to your data, infrastructure, or users.

This is exactly why we are Cyber Essentials and Cyber Essentials Plus certified, and why we have our own in-house cyber security team focused on protecting both our systems and our clients.

TAKING IT GLOBAL, DELIVERING CONSISTENCY ACROSS BORDERS

Our Professional Services team recently travelled to Luxembourg to deliver a full infrastructure refresh for a client site. The project involved replacing legacy servers, switches, and UPS systems, bringing the environment in line with the standards already established across their UK and US operations.

The goal was straightforward. Create a consistent, secure, and supportable IT estate across all locations.

Standardisation like this makes a real difference. It reduces risk, simplifies ongoing support, and ensures every site operates to the same level. It also gives the business a more unified and professional IT footprint globally.

And yes, while the focus was very much on delivery, we suspect there may have been a brief appreciation of the local surroundings along the way.