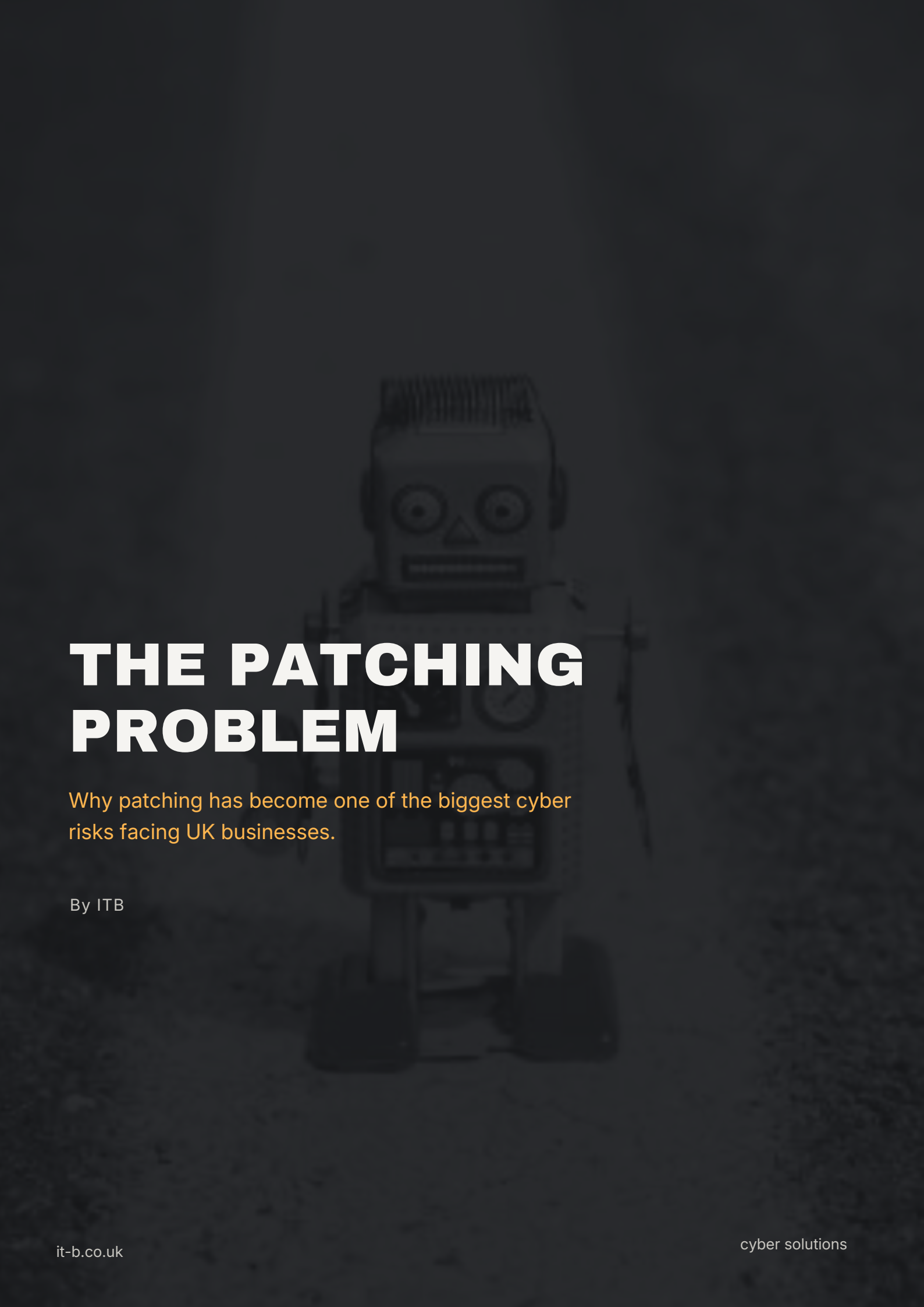

THE PATCHING PROBLEM

Why patching has become one of the biggest cyber risks facing UK businesses.

By ITB

INTRODUCTION

Security has changed.

A few years ago, patching was relatively simple. Windows Update ran in the physical office, systems were updated once a month and most businesses assumed they were covered. One office, push updates, done!

Today, things are very different.

Businesses rely on hundreds of applications, cloud services, laptops, mobile devices and remote users. Attackers are exploiting newly discovered vulnerabilities faster than ever, while AI is helping them identify and target weaknesses at scale.

Patching is no longer just an IT task. It's a business risk.

This guide explains why patching has become more challenging, where organisations commonly fall short and what good patch management looks like in 2026.

THE THREAT

Why attackers love unpatched systems

Cyber criminals don’t need to break down the front door. They look for the side window someone forgot to lock.

Every week, software vendors release security updates to fix newly discovered vulnerabilities. Once those vulnerabilities become public, attackers immediately begin scanning the internet looking for organisations that haven’t installed the fixes.

The longer updates are delayed, the greater the opportunity for attackers. Good patching dramatically reduces that window of opportunity.

KEY TAKEAWAY

Most successful attacks don’t rely on sophisticated hacking — they rely on organisations falling behind on basic security hygiene.

THE MISCONCEPTION

Why Windows Update isn’t enough

One of the biggest misconceptions we see is:

“Windows Update is enabled, so wer’e covered.”

Unfortunately, modern businesses run far more than Windows. Think about everything else that needs updating:

Microsoft 365 Apps	Device drivers
Google Chrome	Network equipment
Microsoft Edge	Firewalls
Adobe Reader	Wi-Fi infrastructure
Java	Third-party business applications
Zoom	VPN software
PDF software	

Without visibility across your entire environment, it’s easy for critical vulnerabilities to remain unnoticed.

STILL RUNNING WINDOWS 10?

Windows 10 reached end of support in October 2025. Any device still running Windows 10 or earlier no longer receives security updates — no patch, however diligent, can fix that. Those systems need replacing or upgrading, not patching.

COMMON MISTAKES

Five patching mistakes we regularly see

01 **Nobody owns patching**

Nobodyhasoverallresponsibility so things can slide.

02 **Critical updates wait for “next month”**

Attackers won’t wait.

03 **Third-party applications are forgotten**

Many vulnerabilities aren’t in Windows itself.

04 **Success isn’t measured**

Installingupdatesisn’tenough.Can you prove every device was successfully patched?

05 **Patching is reactive**

Manyorganisationsonlypatch after hearing about an attack. By then it’s often too late.

THE AI FACTOR

AI has changed the speed of cyber attacks

Artificial Intelligence isn't just helping defenders. It's helping attackers too.

AI enables cyber criminals to:

- Analyse vulnerabilities faster
- Automate reconnaissance
- Identify exposed systems at scale
- Develop attacks more quickly
- Prioritise vulnerable organisations

This means businesses now have less time between a vulnerability becoming public and attackers attempting to exploit it.

SPEED MATTERS.

COMPLIANCE

Where Cyber Essentials fits

Cyber Essentials remains one of the most effective ways for organisations to improve their baseline security. One of its core principles is ensuring supported software is kept up to date.

Good patch management helps organisations:

- ✓ Reduce avoidable cyber risk
- ✓ Meet Cyber Essentials requirements
- ✓ Demonstrate good security practice
- ✓ Build customer confidence

Cyber Essentials is an excellent starting point — but maintaining security requires continual attention, not just an annual certification.

COMPLIANCE

The 14-day challenge

Could your business meet the Cyber Essentials patching requirement?

One of the key requirements of Cyber Essentials is that high-risk vulnerabilities (those rated Critical or High where fixes are available) should normally be remediated within 14 days.

That sounds straightforward. In reality, many organisations struggle to consistently achieve it.

Ask yourself:

- ☐ Could we identify every critical vulnerability today?
- ☐ Would we know which systems are affected?
- ☐ Could we prioritise business-critical assets?
- ☐ Could we deploy the required patches within 14 days?
- ☐ Could we prove it if an auditor or insurer asked?

If you answered “No” or “Not sure” to any of these questions, your organisation may have unnecessary exposure to cyber risk.

KEY TAKEAWAY

The challenge isn’t installing updates. It’s knowing what needs updating, prioritising the right vulnerabilities and proving you’ve done it.

INSURANCE

Cyber insurance is asking tougher questions

Cyber insurance has evolved significantly. It's no longer enough to simply state that updates are installed. Insurers increasingly expect organisations to demonstrate that they have effective security processes in place.

This includes:

Patch management	Real time threat monitoring
Vulnerability management	Incident response planning
Multi-factor authentication	Security awareness

Good security doesn't just reduce risk — it can also strengthen your position during insurance renewals.

THE STANDARD

What good looks like

Modern patch management isn't about installing updates. It's about having confidence.

Organisations with mature patch management typically:

— Know every asset they own

— Understand which vulnerabilities matter most

— Prioritise critical updates

—Patch third-party software

— Monitor compliance

— Report on patch status

— Regularly review security posture

Patching becomes part of an ongoing security programme rather than a monthly task.

SELF-ASSESSMENT

Patch management maturity model

LEVEL	DESCRIPTION
Level 1	Updates are installed manually when someone remembers.
Level 2	Windows Update is enabled across most devices.
Level 3	Patching is monitored and reported.
Level 4	Vulnerabilities are prioritised based on business risk.
Level 5	Patch management forms part of a wider managed security strategy.

Where would you place your organisation today?

SELF-ASSESSMENT

Patch management checklist

Canyou answer YESto allof these?Click each tocheckitoff.

- [ ] Do we know every device connected to our business?
- [ ] Do we know which software is installed?
- [ ] Can we identify critical vulnerabilities quickly?
- [ ] Are critical patches prioritised?
- [ ] Do we patch third-party applications?
- [ ] Can we prove updates have been installed successfully?
- [ ] Are remote workers included?
- [ ] Is someone accountable for patch management?
- [ ] Would we meet Cyber Essentials expectations?
- [ ] Could we confidently answer our cyber insurer's questions?

If you've answered No or Not Sure to any of these, it's worth taking a closer look at your current approach.

itb
cyber solutions

NEXT STEPS

How confident are you in your patch management?

If you're unsure where your organisation stands, a short review can often identify simple improvements that significantly reduce cyber risk.

At ITB, we help organisations move from reactive patching to a more structured, risk-based approach that supports wider security, compliance and business resilience.

Whether you're reviewing your Cyber Essentials readiness, planning for cyber insurance renewal or simply looking to improve visibility, understanding your current position is the best place to start.

Complimentary Patch Health Check

We'll review:

Your current patching approach
Visibility across your environment
Common gaps and risks
Practical recommendations
Next steps based on your organisation — not a generic checklist

BOOK YOUR PATCH HEALTH CHECK

solutions@it-b.co.uk 01865 595 510 it-b.co.uk