

Most SMEs Fail This 5-Minute Security Test

Can Your Business Survive a Cyber Attack Tomorrow?

25+ Years of IT Security & Digital Transformation Consulting | Award-Winning Company | International
Certifications & Accreditations | ICO registered | ISO 9001, ISO 27001 and ISO 45001

Start Here — One Critical Question

If your systems were locked by ransomware tomorrow, how long could your business continue operating?

- ☐ We would continue normally
- ☐ A few hours disruption
- ☐ 1–2 days downtime
- ☐ More than 3 days
- ☐ Not sure

If you selected anything other than the first option, your business is already at risk.

Why SMEs (5–100 Users) Are the Primary Target

Cybercriminals have shifted focus to smaller businesses. The reason is straightforward: SMEs offer maximum impact with minimal resistance.

- Limited internal IT governance — security gaps are easy to exploit
- Over-reliance on basic IT support that does not include cybersecurity
- No structured security framework — reactive rather than proactive
- 43% of all cyber attacks now target small and medium businesses

5-Minute Security Test

Answer honestly — YES, NO, or NOT SURE — for each question below.

1. Endpoint Protection

Question	YES	NO	NOT SURE
Are you still relying mainly on traditional antivirus software?	☐	☐	☐
Do you have advanced threat detection (EDR/XDR) in place?	☐	☐	☐
Are all endpoints — laptops, mobiles and servers — centrally managed and monitored?	☐	☐	☐

Note: Traditional antivirus is obsolete against modern ransomware and account-takeover attacks. Advanced endpoint detection is now the baseline requirement.

2. Backup & Recovery

Question	YES	NO	NOT SURE
Are backups automated and verified daily?	☐	☐	☐
Are backups stored offsite or in an isolated cloud environment?	☐	☐	☐
Are backups protected from deletion (immutable or air-gapped)?	☐	☐	☐
Have you performed a full test restore within the last 90 days?	☐	☐	☐

Note: Most SMEs only discover backup failures during an actual crisis. A backup that has not been test-restored is not a backup — it is an assumption.

3. Ransomware Readiness

Question	YES	NO	NOT SURE
Do you have a documented, multi-step incident response plan?	☐	☐	☐
Can your IT provider walk through this plan clearly and confidently?	☐	☐	☐
Do you know your Recovery Time Objective (RTO) and Recovery Point Objective (RPO)?	☐	☐	☐

Note: If a plan is not written down and tested, it does not exist. A verbal assurance from an IT provider is not an incident response plan.

4. User & Device Control

Question	YES	NO	NOT SURE
Is Multi-Factor Authentication (MFA) enforced across all systems and email?	☐	☐	☐
Are users restricted from installing unauthorised software?	☐	☐	☐

Are all devices encrypted and centrally managed?	☐	☐	☐
Do you have a formal process for joiners, movers and leavers (access control)?	☐	☐	☐

Note: Over 80% of data breaches begin with compromised user credentials. MFA alone blocks the majority of credential-based attacks.

5. Monitoring & Threat Detection

Question	YES	NO	NOT SURE
Is your IT environment monitored around the clock (24/7/365)?	☐	☐	☐
Are real-time alerts and automated response mechanisms active?	☐	☐	☐
Do you have a Security Operations Centre (SOC) or equivalent coverage?	☐	☐	☐

Note: The average breach goes undetected for over 200 days. Without continuous monitoring, you will not know an attack is underway until significant damage has occurred.

6. Independent Security Validation

Question	YES	NO	NOT SURE
Has your IT security been independently audited in the last 12 months?	☐	☐	☐
Are vulnerabilities tested regularly through penetration testing?	☐	☐	☐
Do you have a formal, management-approved security policy in place?	☐	☐	☐

Note: Internal IT teams frequently miss critical gaps. Independent validation is the only objective measure of your true security posture.

Your Risk Score — How Did You Do?

Your Answers	Risk Level	What This Means
Mostly YES	Low-Moderate Risk	You have a reasonable foundation. Professional review will identify hidden gaps.
Mixed Answers	High Risk	Clear vulnerabilities exist. Attackers target businesses at this stage. Act promptly.
Mostly NO / Not Sure	Critical Risk	Your business is highly exposed. The cost of an incident far exceeds prevention.

Where Most SMEs Go Wrong

- Treating standard IT support as cybersecurity — they are fundamentally different disciplines
- Assuming ‘it won’t happen to us’ — SMEs are now the primary target, not large enterprises
- Having backups without a tested recovery plan — backups are worthless if you cannot restore under pressure
- No real-time monitoring — most breaches go undetected for weeks or months
- No MFA enforced — over 80% of breaches begin with compromised login credentials

Why Accel Infotec Ltd?

We operate differently from conventional IT providers. Our focus is protecting your ability to trade, not simply maintaining your technology.

15+ Year old Company

Technology, cybersecurity and Digital transformation since 2009.

Award-Winning & Accredited

Internationally certified with recognised industry accreditations.

International Reach

Operating across the UK, UAE and India — enterprise-grade security for SMEs. Start ups

SME-Focused Approach

Practical, scalable frameworks built specifically for businesses of 5–100 users.

Business Continuity First

We protect your ability to trade — not just your technology.

Core Services

- Cybersecurity Architecture & Risk Management
- Cloud & Infrastructure Security
- 24/7 Monitoring & Threat Detection
- Endpoint & Data Leakage prevention
- Incident Response & Business Continuity Planning
- End-to-End Digital Transformation
- Business Application softwares
- Workforce management softwares
- Technology Audits for ISO standard
- AI readiness audits

Book Your Free 30-Minute Security Audit

Identify your risks before attackers do.

We will assess your current IT and security posture, identify vulnerabilities and exposure points, and provide a clear, prioritised action plan. No obligation. No technical jargon. Just actionable clarity.

Email: sales@accelinfotec.com | **Phone:** 07404 559642 | **Web:** accelinfotec.co.uk

Principle Consultant: syed@accelinfotec.com Support department: support@accelinfotec.com

Most SMEs only take cybersecurity seriously after an incident. By then, the cost is already paid. Do not let your business become a statistic.